Buyer's Guide: Exchange Server Archiving p. 79

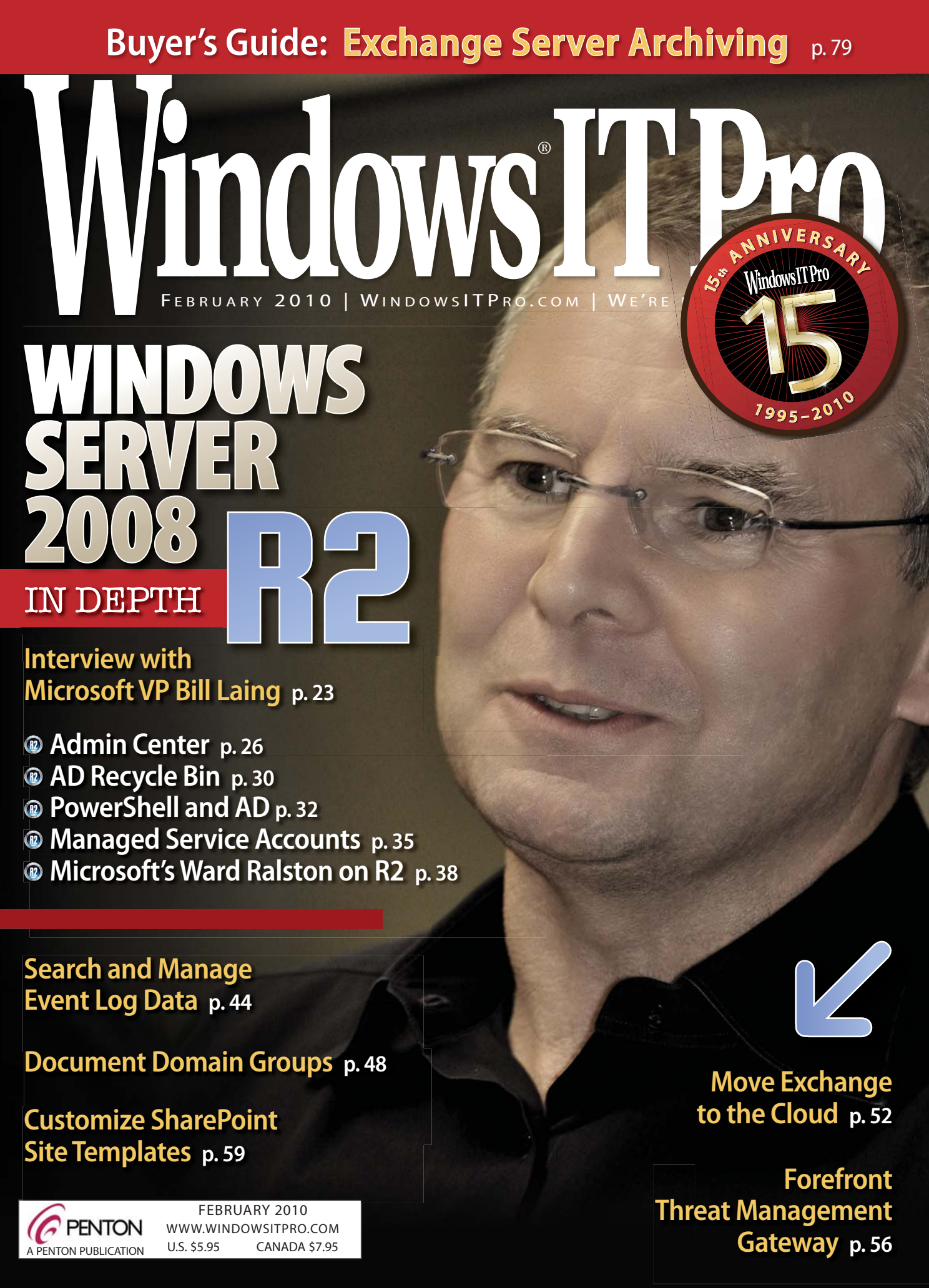
Windows® IT Pro

FEBRUARY 2010 | WINDOWSITPRO.COM | WE'RE

15th ANNIVERSARY Windows IT Pro 15 1995–2010

WINDOWS SERVER 2008 R2

IN DEPTH



Interview with Microsoft VP Bill Laing p. 23

- Admin Center p. 26
- AD Recycle Bin p. 30
- PowerShell and AD p. 32
- Managed Service Accounts p. 35
- Microsoft's Ward Ralston on R2 p. 38

Search and Manage Event Log Data p. 44

Document Domain Groups p. 48

Customize SharePoint Site Templates p. 59

Move Exchange to the Cloud p. 52

Forefront Threat Management Gateway p. 56

PENTON
A PENTON PUBLICATION

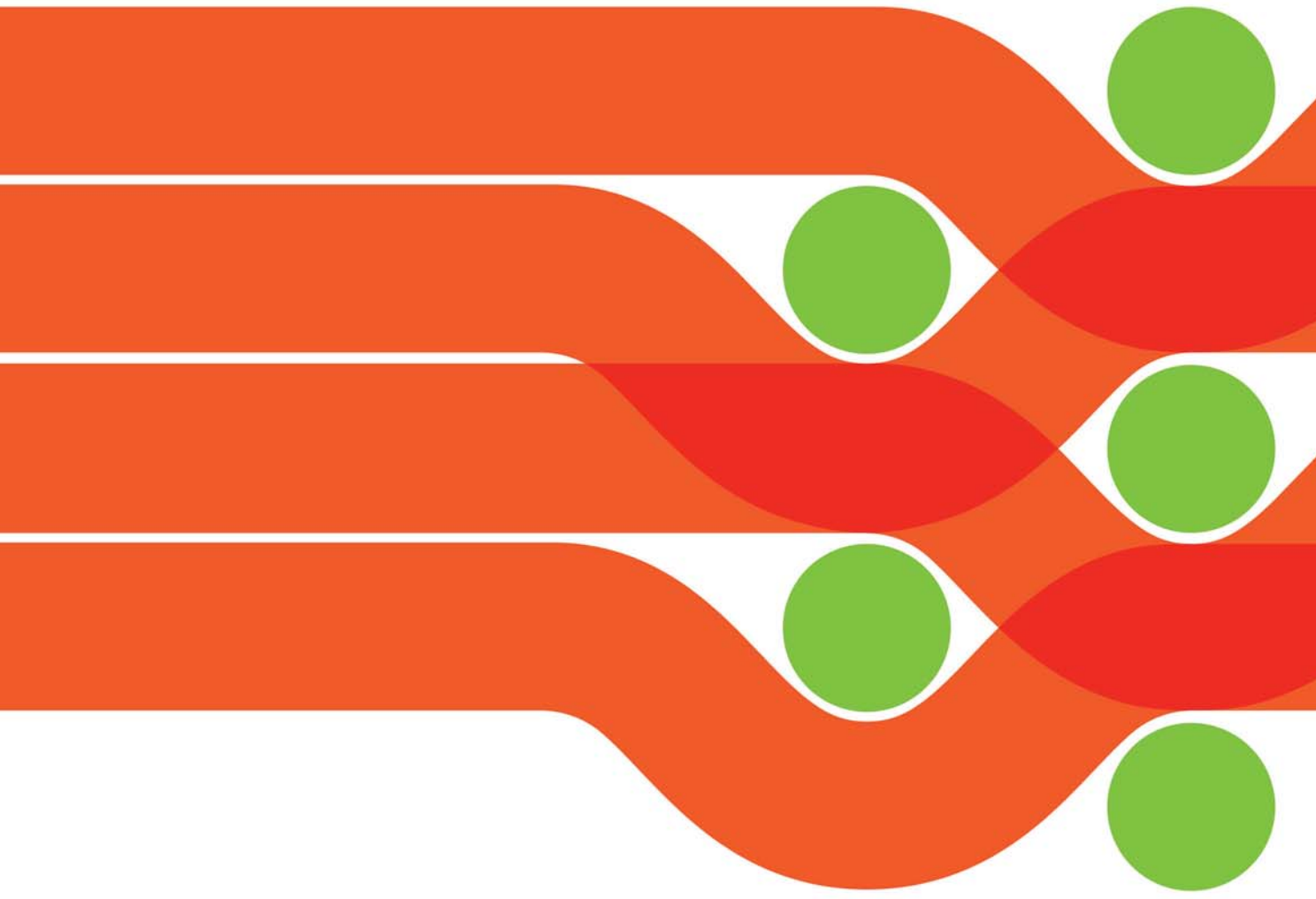
FEBRUARY 2010
WWW.WINDOWSITPRO.COM
U.S. $5.95 CANADA $7.95

Smarter technology for a Smarter Planet:

Building a fluid enterprise.

To date, companies have spent billions of dollars building automated systems to manage vertical business functions—ERP, CRM, etc. Unfortunately, these systems were never designed to talk to each other. Today, the average employee wastes 5.3 hours per week working within these siloed and inefficient processes. IBM's comprehensive business process management solutions connect your disparate processes, enabling fluid workflows. IBM has given over 5,000 companies the visibility and automated processes they need to respond to changing demands and work smarter, from a freight company that reduced development costs by 30% to an oil producer now measuring their fields in real time, doubling the industry's average recovery rates.

A smarter business needs smarter software, systems and services.
Let's build a smarter planet. ibm.com/flexible



C O N T E N T S

COVER STORY

23 What's New in Windows Server 2008 R2

Bill Laing, corporate vice president of Microsoft's Windows Server Division, discusses the release of Windows Server 2008 R2. Laing tells how listening closely to customers and partners yielded a product that helps businesses operate more efficiently in a tight economy.

BY MICHAEL OTEY

26 Using Active Directory Administrative Center in Windows Server 2008 R2

Learn how to manage Active Directory in fewer steps by using ADAC, Microsoft's new task-oriented administration tool, which replaces Active Directory Users and Computers.

BY JAN DE CLERCQ

30 AD Recycle Bin FAQs

The Active Directory Recycle Bin was introduced in Windows Server 2008 R2. Inform yourself about what it is and what you need to do to use it.

BY JOHN SAVILL

32 PowerShell and Active Directory

With the release of Windows 7 and Windows Server 2008 R2, the wait for full-fledged PowerShell Active Directory support is over. Microsoft has shipped an AD module and PowerShell Drive provider in these new releases to make managing AD from PowerShell a snap.

BY DARREN MAR-ELIA

35 Use MSAs to Ease the Pain of Administering Service Accounts

Managed service accounts in Windows Server 2008 R2 can make your life easier when it comes to administering service accounts, SPN delegation, and password management.

BY JOHN SAVILL

38 Why You Need Windows Server 2008 R2

Ward Ralston explains virtualization capabilities, licensing, server roles, AD improvements, and other need-to-know topics related to Windows Server 2008 R2.

BY MICHAEL OTEY

FEATURES

41 Using AD Recycle Bin For Mailbox Recovery

Learn how the Active Directory Recycle Bin and the time-proven tool of logic can make troubleshooting deleted user objects and recovering users in AD easier.

BY J. PETER BRUZZESE

A Free GUI–Based AD Recycle Bin Tool 42

44 How to Efficiently Search and Manage Event Log Data

You can configure Windows to help you deal with event log data and find events before they prove harmful.

BY ORIN THOMAS

48 Document Your Domain Groups

Jim Turner goes beyond the typical group-listing script, providing an admin script that produces a thorough single-domain listing of all your Active Directory (AD) groups in a nicely formatted, easy-to-read layout.

BY JIM TURNER

52 Moving Exchange to the Cloud, Part 2

In determining whether to move email services online, companies must consider hosted email options, user needs, support responsibilities, application integration, and cost. Not all implementations lend themselves to cloud-based services.

BY TONY REDMOND

56 Quickly Respond to Security Threats with Forefront Threat Management Gateway

Taking Forefront Threat Management Gateway out for a quick spin, you can't help but like its new security features including malware blocking at the gateway and the ability to inspect inbound and outbound HTTPS traffic.

BY RUSSELL SMITH

59 Customizing SharePoint Site Templates

Learn how to create custom SharePoint templates by using site templates and site definitions.

BY RON CHARITY

INTERACT

17 Reader to Reader

Use VBScript to prevent scripts from running, troubleshoot Windows XP Pro SP3's annoying audio echo, use NTBackup to back up SharePoint, and learn how to install Windows 7 on a netbook.

21 Ask the Experts

Improve Remote Desktop performance, learn about virtual machine storage options, diagnose Outlook 2007 Business Contact Manager problems, and find out when you can use BitLocker.

IN EVERY ISSUE

5 letters@windowsitpro.com
6 IT Community Forum
87 Directory of Services
87 Advertising Index
87 Vendor Directory
88 Ctrl+Alt+Del

Windows IT Pro
A PENTON PUBLICATION

FEBRUARY_2010
VOLUME_16
NO_2

COLUMNS

CROCKETT | IT PRO PERSPECTIVE

3 Securing Data Wherever Users Roam

An IT director at a 150-user architectural firm explores Microsoft's new Forefront tools—Threat Management Gateway and Unified Access Gateway—for securing data access to web-savvy, mobile workers.

THURROTT | NEED TO KNOW

7 What You Need to Know About Windows Azure and Microsoft Forefront 2010 Products

Windows Azure is much like Windows Server, except that it's hosted by Microsoft at its datacenters and not on premises at your own company. And Microsoft is taking a more holistic approach to security with Forefront 2010.

MINASI | WINDOWS POWER TOOLS

9 Control Windows Features with PowerShell Cmdlets

Windows Server 2008 R2 shakes up the server-configuration process with DISM and three new PowerShell cmdlets. Here's how to make use of those cmdlets.

OTEY | TOP 10

11 New Features in SharePoint 2010

The SharePoint 2010 release will be available only in 64-bit editions, but it adds better search capabilities, enhanced collaboration features, and better browser support.

MORALES | WHAT WOULD MICROSOFT SUPPORT DO?

14 Diagnose Shutdown Problems with Xbootmgr

When a system has shutdown or restart issues, system shutdown statistics can help in resolving the problem. To get this information, use the Windows Performance Toolkit xbootmgr .exe tool, which can help you pinpoint problematic services that occur during shutdown.

COVER PHOTO BY JIM MOLNAR

Access articles online at www.windowsitpro.com. Enter the article ID (located at the end of each article) in the InstantDoc ID text box on the home page.

C O N T E N T S

PRODUCTS

64 New & Improved
Check out the latest products to hit the marketplace.
PRODUCT SPOTLIGHT: DeskCenter Management Suite

REVIEW
65 Paul's Picks
Internet Explorer 9 shows potential; and what is replacing Microsoft Works? (And why should you care?)
BY PAUL THURROTT

REVIEW
66 Mimosa NearPoint for Microsoft Exchange
Its price might scare away smaller businesses, but this archiving and eDiscovery product provides a lot of value for those who need it.
BY J. PETER BRUZZESE

REVIEW
68 Sendio ESP 360
Sendio's E-mail Security Platform (ESP) sits on your network in front of your mail servers, protecting them from both spam and malware.
BY NATHAN WINTERS

COMPARATIVE REVIEW
69 4 Active Directory Management Tools
These four products—Ensim Unify Enterprise Edition, ManageEngine ADManager Plus, NetIQ Directory and Resource Administrator, and Quest Software ActiveRoles Server—help you gain control of your AD infrastructure.
BY ERIC B. RUX

MARKET WATCH
75 Understanding Microsoft's Virtualization Technologies
What are the differences between Microsoft's Hyper-V, App-V, and MED-V solutions? Which one is right for you? Here's how to navigate Microsoft's virtualization maze.
BY MICHAEL OTEY

BUYER'S GUIDE
79 Exchange Server Archiving for E-Discovery
Archiving presents both technical problems and legal problems. Learn what you need to create a reliable and legal archiving system.
BY B. K. WINSTEAD

82 Industry Bytes
Why Motorola's DROID might be the ultimate smartphone, the top ten things about Exchange 2010, and one foolproof, 5-step hiring process.

Windows IT Pro

EDITORIAL

Editorial and Custom Strategy Director
Michele Crockett mcrockett@windowsitpro.com

Executive Editor, IT Group
Amy Eisenberg amy@windowsitpro.com

Technical Director
Michael Otey motey@windowsitpro.com

Custom Group Editorial Director
Dave Bernard dbernard@windowsitpro.com

Web and Developer Strategic Editor
Anne Grubb agrubb@windowsitpro.com

Systems Management
Karen Bemowski kbemowski@windowsitpro.com
Caroline Marwitz cmarwitz@windowsitpro.com
Zac Wiggy zwiggy@windowsitpro.com

Messaging , Mobility, SharePoint, and Office
Brian Keith Winstead bwinstead@windowsitpro.com

Networking and Hardware
Jason Bovberg jbovberg@windowsitpro.com

Security
Lavon Peters lpeters@windowsitpro.com

SQL Server
Megan Bearly Keller mkeller@windowsitpro.com
Sheila Molnar smolnar@windowsitpro.com

Production Editor
Brian Reinholz breinholz@windowsitpro.com

IT Media Group Editors
Linda Harty, Chris Maxcer, Rita-Lyn Sanders

CONTRIBUTORS

News Editor
Paul Thurrott news@windowsitpro.com

SharePoint and Office Community Editor
Dan Holme danh@intelliem.com

Senior Contributing Editors
David Chernicoff david@windowsitpro.com
Mark Joseph Edwards mje@windowsitpro.com
Kathy Ivens kivens@windowsitpro.com
Mark Minasi mark@minasi.com
Paul Robichaux paul@robichaux.net
Mark Russinovich mark@sysinternals.com

Contributing Editors
Alex K. Angelopoulos aka@mvps.org
Sean Deuby sdeuby@windowsitpro.com
Michael Dragone mike@mikerochip.com
Jeff Fellinge jeff@blackstatic.com
Brett Hill brett@iisanswers.com
Darren Mar-Elia dmarelia@windowsitpro.com
Tony Redmond tony.redmond@hp.com
Ed Roth eroth@windowsitpro.com
Eric B. Rux ericbrux@whshelp.com
John Savill john@savilltech.com
William Sheldon bsheldon@interknowlogy.com
Randy Franklin Smith rsmith@montereytechgroup.com
Curt Spanburgh cspanburgh@scg.net
Orin Thomas orin@windowsitpro.com
Douglas Toombs help@toombs.us
Ethan Wilansky ewilansky@windowsitpro.com

ART & PRODUCTION

Senior Art Director
Larry Purvis lpurvis@windowsitpro.com

Art Director
Layne Petersen layne@windowsitpro.com

Production Director
Linda Kirchgesler linda@windowsitpro.com

Senior Production Manager
Kate Brown kbrown@windowsitpro.com

Assistant Production Manager
Erik Lodermeier erik.lodermeier@penton.com

ADVERTISING SALES

Publisher
Peg Miller pmiller@windowsitpro.com

Director, International and Agency Services
Don Knox don.knox@penton.com

EMEA Managing Director
Irene Clapham irene.clapham@penton.com

Director of IT Strategy and Partner Alliances
Birdie J. Ghiglione birdie.ghiglione@penton.com, 619-442-4064

Online Sales and Marketing Manager
Dina Baird Dina.Baird@penton.com

Key Account Directors
Jeff Carnes jeff.carnes@penton.com 678-455-6146
Chrissy Ferraro christina.ferraro@penton.com 970-203-2883

Account Executives
Barbara Ritter barbara.ritter@penton.com 858-759-3377
Cass Schulz cassandra.schulz@penton.com 858-357-7649

Client Project Managers
Michelle Andrews 970-613-4964
Kim Eck 970-203-2953

Ad Production Supervisor
Glenda Vaught glenda.vaught@penton.com

MARKETING & CIRCULATION

Customer Service 800-793-5697 (US and Canada) 44-161-929-2800 (Europe)

IT Group Audience Development Director
Marie Evans marie.evans@penton.com

Marketing Director
Sandy Lang sandy.lang@penton.com

CORPORATE

PENTON

Chief Executive Officer
Sharon Rowlands Sharon.Rowlands@penton.com

Chief Financial Officer/Executive Vice President
Jean Clifton jean.clifton@penton.com

TECHNOLOGY GROUP

Senior Vice President, Technology Media Group
Kim Paulsen kpaulsen@windowsitpro.com

WRITING FOR *WINDOWS IT PRO*
Submit queries about topics of importance to Windows managers and systems administrators to articles@windowsitpro.com.

LIST RENTALS
Contact Walter Karl, Inc. at 2 Blue Hill Plaza, 3rd Floor, Pearl River, NY 10965 or www.walterkarl.com/mailings/pentonLD/index.html.

REPRINTS
Diane Madzelonka, Diane.madzelonka@penton.com, 216-931-9268, 888-858-8851

Crockett

"Microsoft's security tools help IT pros manage complicated scenarios with fewer resources."

Securing Data Wherever Users Roam

Forefront tools provide secure data access

All seemed quiet on the security front at Microsoft until last fall, when the company announced several new products in rapid succession. Amid the noise surrounding Windows 7 and Windows Server 2008 R2, Microsoft quietly strengthened its case for its new positioning—providing "business-ready security"—by introducing Forefront Protection for Exchange, followed closely by Forefront Threat Management Gateway (TMG) 2010 and Forefront Unified Access Gateway (UAG) 2010. TMG lets companies provide safe web browsing to users. UAG gives users secure remote access to business resources.

George Podolak, director of IT at New York-based architectural firm Pei Cobb Freed & Partners, recently talked about the challenges he faced as one of a two-member IT team supporting 150 web-savvy users serving security-conscious clients such as high-profile banks and the Louvre Museum in Paris.

"We work with people who are very cognizant of their data and they don't want their information—preliminary drawings, for example—splashed on the Internet," Podolak said. "We've always had a good perimeter defense. We regulate very well what comes in. But the thing that has always bothered me is egress—anyone could go out to a malware site and infect the entire system."

Podolak said that he's always taken a fairly liberal stance with regulating users' access to the Internet. "We have really smart kids coming in here and they're used to using Facebook. It would be easy to say we're just going to cut off Facebook for everybody, but that's sort of counterproductive. It's not Facebook I'm worried about, it's what you can access from Facebook."

After using or evaluating various point solutions for years, Podolak adopted Microsoft's Forefront TMG and Forefront UAG solutions in the Technology Adoption Program (TAP). John (JG) Chirapurath, Microsoft's director of the identity and security business group, explained how these solutions fit with Microsoft's three-pronged security strategy. "We're focused on three things," Chirapurath said. "One is the ability to protect data and let users access it anywhere. Second is ensuring that security is integrated but extensible. Third is that security is simple to deploy and easy to manage."

Chirapurath said that one of the key tenets of Microsoft's business-ready security strategy is helping IT pros resolve the "tension between being protective and granting access." Chirapurath pointed out the increase in web use in businesses, and the commensurate increase in corporate exposure to malware. He also noted that phishing rose in the first half of 2009, according to a Microsoft Security Intelligence Report. TMG, which was based on ISA Server 2006, provides URL filtering, anti-malware, and intrusion-prevention technologies combined with firewall and VPN protection. Chirapurath said that TMG is the first product to rely on cloud computing technology—it uses Microsoft Reputation Services, a Microsoft-hosted cloud-based system that maintains a database that helps protect customers from malicious sites. UAG helps IT pros grant mobile workers access to business resources through PCs and mobile devices by supporting Windows DirectAccess, which enables seamless, always-on connectivity.

Echoing the constant refrain of IT pros in the economic downturn, Podolak said that Microsoft's Forefront products helped him consolidate his security toolkit. "I was looking at different technologies for everything—email filtering, URL filtering," Podolak said. "I needed a comprehensive strategy for dealing with all the threats, and a console, and the ability to produce reports so I could prove to clients that we have a secure system."

Chirapurath said that the Forefront tools are appropriate for companies large and small primarily because they're easy to use, one of the legacies of their ISA Server roots. Chirapurath called ISA Server "one of those products that was loved across the board because it was "easy to deploy and easy to use."

Although Podolak said that his company is among the smallest in Microsoft's pilot program, he's observed that the security problems faced by his small company and large enterprises are essentially the same. Although the price of the Forefront tools was competitive, he felt that the reason the products were compelling for small companies was because they were easy to use. For companies with small IT organizations and unlimited resources, simplified management can trump lots of other considerations, Podolak said. "We have the same problems, but it's even more difficult because we have less staff."

If Podolak's early assessment is any indication, Microsoft's new security tools follow an ongoing trend of helping IT pros manage increasingly complicated scenarios with fewer resources.

InstantDoc ID 103312

MICHELE CROCKETT (michele.crockett@penton.com) helped launch *SQL Server Magazine* in 1999, has held various business and editorial roles within Penton Media, and is currently editorial and custom strategy director of *Windows IT Pro, SQL Server Magazine,* and *System iNEWS.*

Prime Your Mind

with Resources from Left-Brain.com

Left-Brain.com is the online superstore stocked with educational, training, and career-development materials focused on meeting the needs of IT professionals like you.

Featured Product:

VMware vSphere Training

VMware vSphere Training courseware is appropriate for both new VMware administrators and those who are preparing for the VCP certification. Besides completely covering how to administer a VMware infrastructure, this course also reviews third-party solutions that are widely used by the virtualization community. Find out more about this course and other virtualization resources at Left-Brain.com

windowsitpro.com/go/left-brain/vsphere

left-brain

*Plus shipping and applicable tax.

www.left-brain.com

Windows IT Pro

- Large File Transfers
- Thin-Client Benefit
- Business Value
- Model FAQ

LETTERS@WINDOWSITPRO.COM

Large File Transfers

I enjoyed reading Michael Morales' What Would Microsoft Support Do? column, "Disk2vhd: The Windows Troubleshooter's New Best Friend" (December 2009, InstantDoc ID 102980). But I thought of one potential problem that Michael didn't elaborate on.

After using the Disk2vhd utility to create a VHD out of a physical machine, how do you suggest getting those potentially multi-gigabyte VHD files back and forth? Michael mentioned folks sending the VHD files to Microsoft for support cases. I'm wondering how to accomplish this file transfer and whether Michael's procedure can be used outside Microsoft. I'm trying to come up with some method to receive, say, a customer's VHD without utilizing FTP. I suppose the customer could always overnight a portable USB drive.

—Michael Dragone

Not long ago, Microsoft had a single large FTP site where customers could upload their dump files and data. Now, engineers working on a customer's issue can create an online workspace that customers access via a web browser. The workspace is a Microsoft facility. I don't know the file-size limitations placed on these workspaces, but I do know that we've received 60GB dumps before.

Sometimes, we go the route you mentioned and have customers send us USB drives containing the image and/or data. Then we send them back. We've had customers send us whole machines in the past—but not as often these days with virtualization technology. There might be some places online, such as SkyDrive (skydrive.live.com), that can help with your needs.

—Michael Morales

To Deploy or Not to Deploy

I read Michele Crockett's IT Pro Perspective editorial, "To Deploy or Not to Deploy" (December 2009, InstantDoc ID 102993), in which she asked, "What makes the most sense for your company in this launch wave?" I'm an IT director for a private, non-profit social services/healthcare company of about 600 employees. We've been using a thin-client environment since 2004. Approximately 95 percent of our employees use refurbished Wyse Winterm clients that I bought online for about $100 each. Before I convinced management to go this direction, our staff was sharing computers at about a seven-to-one ratio. The thin-client solution has worked well and helped us meet our goal of giving all our users a computer on their desk—which was necessary for the successful adoption of our Electronic Health Record (EHR).

Considering the growing number of multimedia sources—and the fact that we could save a lot of money in mileage reimbursement—I'm looking at the Intel Atom processor and application virtualization as the next phase of our server/desktop environment. We've been looking at systems that we can build for about $150. We own more than 400 Windows XP licenses and have a lot of IDE drives left over from when we had more desktops. I'd like to virtualize the applications that I want to centrally manage. These thin-client hybrids will go to managers and meeting rooms. I plan to use the freeware tool TrueCrypt (www.truecrypt.org) to encrypt the hard drive; locally install Microsoft Office, ShoreTel Personal Call Manager, Mozilla Firefox; and virtualize the EHR. Our treatment rooms will probably always use a true thin-client appliance, with a digital signature pad attached. It sounds to me as if Windows Server 2008 R2 and Windows 7 are pretty nice OSs and have a lot to offer. But I just don't see them as crucial to my strategy at the moment.

—Nate McAlmond

In Michele Crockett's article, "To Deploy or Not to Deploy," Matt Becker listed many factors that my company and its customers are considering. In this tough economic climate—many companies resorting to layoffs, and 2010 looking like another tough year—the prospect of meshing technology upgrades, refreshes, enhancements, and training with already strained or reduced budgets is daunting.

The key decision factor, regardless of the state of the economy, has to be business value. Unfortunately, these days, many IT people are neglecting to examine business value before launching a new technology; they've forgotten that money is no longer free-flowing. Making a strong business case for how an upgrade or rollout will help the business's bottom line is always essential, and even more so now.

A positive increase in the bottom line can happen in many ways, some tangible and some harder to grasp. Return on investment (ROI), support and maintenance costs (yes, all systems still need maintenance), and training costs are tangibles that you can calculate and measure comparatively. However, increased efficiency (resulting from new technologies), transforming the information flow, and streamlining workflow processes might not be as easy to measure. And yet those intangibles—along with improving customer offerings while maintaining superb customer-service levels—should be some of our most important decision-making benchmarks. For that reason, Windows 7, Server 2008 R2, and SharePoint—at a minimum—are on our horizon.

In tough times, it's wise to be poised to grow the business when the economy does rebound. Those who keep investing and advancing their technologies will benefit from being "ready to go" when the workload increases.

—Kristy Hartman Mumma

Model FAQ

John Savill's FAQ, "Should I use folder redirection or roaming profiles in Remote Desktop, Virtual Desktop Infrastructure (VDI), and other environments?" (InstantDoc ID 103150) is a model of how to explain a complex subject clearly and succinctly. I finished reading it almost before I realized I'd started reading it! Bravo!

—Philip Herlihy

Windows IT Pro welcomes feedback about the magazine. Send comments to letters@windowsitpro.com, and include your full name, email address, and daytime phone number. We edit all letters and replies for style, length, and clarity.

Read on twitter

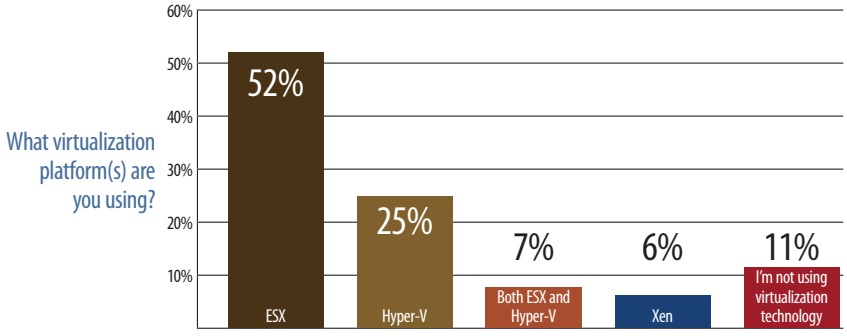
MojaveMedia Stop blaming your #Exchange server for your inability to print a Word doc, unless Exchange is your print server. That's a different problem! December 9, 2009

MojaveMedia Ask and you shall *sometimes* receive. Microsoft reconsiders support for Exchange 2007 on Windows 2008 R2. http://msexchangeteam.com/archive/2009/11/04/453026.aspx November 4, 2009

And Now for Something Really Geeky: R2 Haiku

Microsoft ran a contest for the best haiku about Windows Server 2008 R2. By the time you read this, the top entries and winner will be posted at www.r2haiku.com.

Instant Poll Results:
Virtualization Platform Choices



From the Forums at www.windowsitpro.com

Readers are interacting online in our blogs, forums, and articles. Here, we present some excerpts of their comments unedited and in their own words.

Windows 7

Surf40: *I desperately need to solve this grave problem. My Windows 7 workstations get locked out of the domain when a user locks a machine. Embarrassingly enough, this is happening to Admin accounts. Initial logon from a powered-off state in the AM works fine. But the minute we lock a machine here in the IT department, or logon to another Windows XP workstation, the account (that is concurrently logged onto his Windows 7 PC) gets locked out. The domain controllers' Security event viewer log is generating 675 and 680 errors. I have the users' accounts, that are logging into Windows 7 boxes first thing in the AM, being audited.*

MikeKnight: *What server are you using? 2000/2003/2008? Either way, on your workstation, try this the next time it happens:*

1. *Remove passwords by clicking on Start > Run > type "rundll32.exe keymgr.dll, KRShowKeyMgr" and then delete the Domain-related passwords*
2. *Remove passwords in Internet Explorer > Tools > Internet Options > Content > Personal Information > Auto Complete > Clear Passwords*
3. *Delete cookies in Internet Explorer > Tools = Internet Options > General*
4. *Disconnect (note the path before disconnecting) all networks drives, reboot, then map them again*

More often than not it is an explicit drive mapping.

Thurrott

"In real-world terms, it's hard to know how Microsoft's Azure pricing will affect customers. Even the company admits that the current pricing model is almost experimental."

What You Need to Know About Windows Azure

In late 2008, when Microsoft announced sweeping plans to move its server product line to the cloud, few outside the company's Windows Server division even understood what this change in strategy meant for the company and its customers. Now, just over a year later, Microsoft has delivered the first non-beta versions of its core cloud server products, Windows Azure and SQL Azure. And while a hosted version of SQL Server might seem like a fairly obvious solution, a hosted version of Windows Server is a bit more mysterious. Here's what you need to know about Windows Azure.

Azure is a New Platform

Put simply, Windows Azure is the Windows Server OS redesigned as a cloud-based service. At a very high level, Windows Azure is much like Windows Server, except that it's hosted by Microsoft at its datacenters and not on premises at your own company. That is, it provides a platform on which developers can create hosted applications and companies can run hosted applications and store data in the cloud.

But Windows Azure isn't simply the current version of Windows Server modified to work in the cloud. Yes, Microsoft did of course start with a Windows Server core to create Windows Azure, but the system was also designed from the start to work as a cloud-hosted service. As such, Windows Azure and Windows Server both have capabilities that are uniquely their own. According to Microsoft, the company will continue developing each product separately, all the while bringing the respective capabilities of each system closer together. That said, because of their unique focuses, it's likely that they will never truly mirror each other fully.

Another important aspect of Windows Azure is that it works within Microsoft's notion of a hybrid computing model, letting companies utilize on-premises servers for those tasks that need to be hosted onsite and cloud-hosted services for those that do not. This system can also be utilized to slowly move resources to the cloud over time as you evaluate the cost, effectiveness, and convenience of such a strategy.

Why Windows Azure?

If Windows Azure were simply a hosted version of Windows Server, the value proposition would be simple to understand but basic in functionality. But as I alluded to earlier, Windows Azure provides a set of benefits that are unique to this platform.

One such benefit involves so-called "spiky" workloads. The canonical example is an online store that experiences typically predictable traffic during most of the year but then far more unpredictable ("spiky") traffic during the holidays. You could purchase additional computing resources to handle the spikes, but these resources would sit idle for much of the time. You could partially offset the spiking by moving to a virtualized infrastructure where many workloads are typically virtualized but then migrated to physical hardware when required; this requires architecting, deploying, managing—and paying for—a very complex infrastructure, however.

With Windows Azure, you can simply add capacity when it's needed. You pay for what you use, when you use it.

For those interested in the hybrid approach, Windows Azure also supports a new composite application model via the Windows Azure platform AppFabric technologies. Through AppFabric, developers can build and manage applications that run on premises but access and cache Azure-based resources.

Pricing and Availability

Microsoft understands that it will likely be some time before enterprises trust their mission-critical workloads to an offsite hosted service such as Azure, so it hasn't yet provided a comprehensive set of pricing and licensing options. Instead, it offers a consumption-based pricing model: Compute resources cost 12 cents an hour, storage is 15 cents per gigabyte stored per month, storage transactions are 1 cent for each 10KB, and data transfers are 10 cents per gigabyte inbound and 15 cents per gigabyte outbound.

For AppFabric usage, Microsoft charges 15 cents per 100,000 messages, and data transfers are 10 cents per gigabyte inbound and 15 cents per gigabyte outbound. SQL Azure incurs additional consumption costs as well.

Microsoft's service level agreement (SLA) states that customers who deploy two or more role instances in different fault and upgrade domains will see external connectivity of 99.95 percent for Internet-facing roles. This is less than the traditional 99.99 percent uptime promise one typically sees with online services, including Microsoft's own Business Productivity Online Suite (BPOS) products.

In real-world terms, it's hard to know how Microsoft's Azure pricing will affect customers. Even the company admits that the current pricing model is almost experimental. That, of course, makes the Windows Azure early adopter process even dicier than it might be otherwise.

Recommendations

As a relatively new and unknown technology, Windows Azure will likely be adopted slowly by established enterprises and more

quickly by new, smaller businesses. But it deserves investigation, regardless of your circumstances, and as Microsoft moves to a more mature pricing model, Azure will likely get even more attractive. Most larger businesses will always have a need to host some resources on premises. The hybrid model offered by Windows Azure and Microsoft's other online services isn't a stopgap: It's a peek into the future of computing.

InstantDoc ID 103270

What You Need to Know About Microsoft Forefront 2010 Products

Over the past few months, Microsoft has upgraded much of its Forefront family of enterprise security products to the latest 2010 versions. These new products include Forefront Protection 2010 for Exchange Server, which shipped in November, and Forefront Threat Management Gateway (TMG) 2010 and Forefront Unified Access Gateway (UAG) 2010, which shipped in December. In the first half of 2010, Microsoft will add Forefront Protection 2010 for SharePoint and Forefront Identity Manager 2010. Here's what you need to know about Microsoft Forefront 2010.

Forefront Protection 2010 for Exchange Server

As with previous versions of Forefront Security, Forefront 2010 Protection 2010 for Exchange Server provides multi-engine protection against malware like viruses, worms, spyware and spam. The difference this time around is performance: In previous Forefront versions, enabling too many anti-malware engines could bog down the server, and administrators were often forced to micromanage the server by proactively enabling different engines that they felt met their needs.

In Forefront Protection 2010 for Exchange Server, the server automatically picks the most effective anti-malware engine for the content in question. It does so based on three different algorithms that examine the size of each message instead of treating each message as a blob as in the past. This way, admins can safely enable multiple engines and be sure that Forefront will use only the appropriate engines intelligently.

For scripting gurus, Forefront Protection 2010 for Exchange Server also picks up full Windows PowerShell compatibility, so you can easily query and control the server from a command line or scripts.

Forefront Threat Management Gateway 2010

Microsoft Forefront Threat Management Gateway (TMG) 2010 is the company's premier endpoint security solution, protecting against viruses, malware, information loss, data theft, and other electronic attacks as well as against emerging threats.

TMG 2010 builds on ISA Server 2006. But it provides new capabilities around web security, URL filtering, web antivirus and malware inspection, and even HTTPS inspection (where ISA could inspect only HTTP). HTTPS inspection requires TMG 2010 to act as a certificate authority, decrypting HTTPS traffic, inspecting the contents, re-encrypting it, then passing it along. Microsoft says that there's enough latency in HTTPS traffic already that the addition of TMG 2010 is unnoticeable. (HTTPS causes a five to 10 percent performance hit over HTTP regardless.) TMG 2010 also provides a simplified management console with a rules- or scenario-based UI and wizards.

Forefront Unified Access Gateway 2010

Forefront Unified Access Gateway (UAG) 2010 (formerly Intelligent Application Gateway) provides secure remote access services for managed and unmanaged PCs and mobile devices. It's typically implemented as an appliance or server that sits in a network DMZ and publishes access to back-end resources such as files, for employees on the go, partners, and even customers. Access occurs via web browser.

UAG queries devices that are attempting to connect to the network and supplies a verdict about the system's health. For managed PCs, this can be quite granular, but even unmanaged systems—including web kiosks—can be granted different levels of policy-based access. For example, if a user at a public web kiosk tries to access the corporate web mail or SharePoint site, you can choose to allow that access, but not allow the sending of attachments. These policies don't just apply to Microsoft servers, either: The company provides built-in policies for several known business solutions, including PeopleSoft and Oracle, and of course you can build your own.

UAG also integrates with new remote access solutions such as DirectAccess, which is part of Windows Server 2008 R2. But it also works with non-Server 2008 R2 servers as well as non-Windows 7 clients, the latter of which might be using some kind of VPN. This includes PCs running Windows XP or Windows Vista as well as PDAs and smart phones based on Windows Mobile.

Recommendations

Microsoft's Forefront family has always provided capable, end-to-end security solutions for enterprises. With the 2010 editions of these products, Microsoft is taking a more holistic approach to security and anticipating the day-to-day scenarios that will become common as more employees work remotely and as companies seek ways in which to open up parts of their infrastructure to outside partners and customers. Other companies may offer compelling individual solutions, but none match the integrated functionality of Forefront.

InstantDoc ID 103271

PAUL THURROTT (thurrott@windowsitpro.com) is the news editor for *Windows IT Pro*. He writes a weekly editorial for *Windows IT Pro UPDATE* (www.windowsitpro.com/email) and a daily Windows news and information newsletter called *WinInfo Daily UPDATE* (www.wininformant.com).

Minasi

"PowerShell doesn't perpetuate the silly division of "stuff the server can do" into *roles* versus *features*."

Control Windows Features with PowerShell Cmdlets

PowerShell brings a little something extra to the process

Windows Server 2008 changes the process of server configuration, thanks to a big GUI shift and to the addition of two new command-line tools (OCSetup and Servermanagercmd) that let you add or remove features. Last month, I noted that with the advent of Server 2008's replacement, Server 2008 R2, Microsoft shook things up even further by deprecating Servermanagercmd and OCList, replacing them with two even newer commands: Deployment Image Servicing and Management (DISM) and three new PowerShell cmdlets. Last month's column covered DISM, so now let's look at the PowerShell offerings.

Server 2008 R2 ships with a PowerShell 2.0–compatibile module called ServerManager that adds three PowerShell cmdlets: *add-windowsfeature*, *get-windowsfeature*, and *remove-windowsfeature*. Their function closely approximates what the *dism /online /enable-feature*, *dism /online /get-features*, and *dism /online /disable-feature* commands do, but they add some of that characteristic extra functionality that we've come to expect from PowerShell cmdlets.

Before running the cmdlets, you'll need to start up an elevated PowerShell prompt (right-click the blue PowerShell icon, choose *Run as Administrator*, and confirm the User Account Control—UAC—prompt) and type

```
import-module servermanager
```

Then, you can get started with the Server Manager cmdlets by typing

```
get-windowsfeature
```

which produces a list of roles, role services, and features, all under the label *features*. (Like DISM, PowerShell thankfully doesn't perpetuate the silly division of "stuff the server can do" into *roles* versus *features*.) Each list entry contains the special name that you need to use if you want to enable or disable that feature.

```
[ ] DHCP Server    DHCP
[X] DNS Server     DNS
[ ] Fax Server     Fax
[ ] File Services  File-Services
[ ] File Server    FS-FileServer
```

The single *X* next to DNS Server specifies that I have the DNS Server role installed on the system and that I *don't* have the DHCP Server, Fax Server, File Services, and File Server role services installed. (A role service is, in Server 2008 R2 parlance, "just a part of a role.") The names on the right are the exact names that you'd feed into the *next* Server Manager cmdlet, *add-windowsfeature*. The syntax of

```
add-windowsfeature fs-fileserver
```

probably doesn't surprise you—so far, it's similar to last month's DISM example, and it's pretty intuitive.

But you *will* be pleasantly surprised about a few other aspects this command. First, notice that the *get-windowsfeature* command reported that the role service's name is *FS-FileServer*, not *fs-fileserver*, as I typed. Remember that annoying insistence on particular uppercase and lowercase in DISM's "magic names" for roles and features? PowerShell doesn't impose that irritation. Second, you can install more than one feature by merely separating them with commas, as in

```
add-windowsfeature dhcp, fax, file-services
```

Compare that simple list-formatted syntax to DISM's irritating need to prefix every feature with /featurename, and you'll start liking the Server Manager cmdlets.

To remove a feature from a server, use the *remove-windows feature* cmdlet, with the same options as *add-windowsfeature:*

```
remove-windowsfeature dhcp, fax
```

The *remove-windowsfeature* and *add-windowsfeature* cmdlets include two more useful options: *-restart* and *-whatif*. PowerShell users will know that *-whatif* appears on just about any PowerShell cmdlet that might undesirably modify your system. This option causes the PowerShell cmdlet to make no actual changes but instead to report what it will do if you leave -whatif off. It ranks as one of my favorite PowerShell features: Nerf bumpers for administrators!

Finally, when added to *add-windowsfeature* or *remove-windows feature*, the -restart option authorizes PowerShell to reboot to complete your addition or removal.

If you haven't yet given PowerShell a try, the Server Manager cmdlets are a gentle introduction to a helpful set of command-line tools. Next month, I'll reveal more of the cmdlets' power.

InstantDoc ID 103282

MARK MINASI (www.minasi.com/gethelp) is a senior contributing editor for *Windows IT Pro*, an MCSE, and the author of 25 books.

Otey

"Like the majority of new Microsoft servers, SharePoint 2010 will ship only as a 64-bit product."

New Features in SharePoint 2010

An integrated Best Practices Analyzer, FAST Search capability, and improved browser support make this release better than ever

Microsoft is releasing a slew of new technologies in 2010, and one of the most important of them is SharePoint 2010. Previously known by the code name SharePoint 14, SharePoint 2010 marks a significant upgrade to the SharePoint product. Here are ten of the most important things about the SharePoint 2010 release, which is expected to be available in the first half of 2010.

10 **New SharePoint editions**—In an effort to better unify the SharePoint lineup, Microsoft will make some big changes to the SharePoint editions with the 2010 release. Windows SharePoint Server (WSS) is gone, and so is Microsoft Office SharePoint Server (MOSS). The free WSS has been replaced by the new SharePoint Foundation 2010. MOSS is replaced by SharePoint Server 2010, which will be available in either the Standard or Enterprise edition as well as in editions for strictly internal sites and for Internet or extranet sites.

9 **New hardware requirements**—Like the majority of new Microsoft servers, SharePoint 2010 will ship only as a 64-bit product. If you're deploying SharePoint on new hardware, this situation shouldn't be a problem, but it's definitely a consideration if you're planning to upgrade an existing SharePoint server.

8 **New software requirements**—In addition to new hardware requirements, SharePoint 2010 will require an x64 edition of either Windows Server 2008 or Server 2008 R2. It also requires a 64-bit version of Microsoft SQL Server 2008 or SQL Server 2005.

7 **SharePoint Best Practices Analyzer**—With the SharePoint 2010 release, SharePoint Best Practices Analyzer will be incorporated as part of the base SharePoint product. This tool provides Microsoft's guidance for SharePoint implementation and troubleshooting. A *Problems and Solutions* page in the analyzer helps you solve common implementation problems.

6 **FAST Search**—The new SharePoint release will incorporate the FAST Search technology that Microsoft acquired from the Norway-based Fast Search & Transfer company. The FAST technology provides a superset of the original SharePoint search capabilities. As its name implies, FAST Search is designed for high-end scalability. It supports a number of enhanced capabilities, including a content-processing pipeline, metadata extraction, visual search, and advanced linguistics.

5 **Usage reporting and logging**—SharePoint 2010 includes a new database designed to support usage reporting and logging. The usage database is extensible, allowing third-party vendors to create custom reports based on the information it contains.

4 **Visio Services**—Visio Services in SharePoint 2010 lets users share and collaborate on Visio diagrams. A built-in viewer lets SharePoint users view Visio files in their browser without having Visio installed on their system. Visio Services also retrieves and renders any external data used in the Visio diagrams.

3 **Enhanced collaboration features**—SharePoint 2010 supports tagging content as well as providing enhanced blog authoring capabilities. There's a new group authentication feature that's based on distribution list or organization and a new rich text editor for creating wikis. In addition, calendars from Microsoft Exchange Server can be merged with SharePoint calendars.

2 **New browser support**—SharePoint 2010 supports an extended set of browsers. It's designed to support XHTML 1.0–compliant browsers and will support Internet Explorer (IE) 8.0 and IE 7.0, Firefox, and Safari. Notably, IE 6.0 isn't supported. So far, there's been no official mention of Google Chrome or Opera.

1 **Enhanced SharePoint Designer**—Microsoft SharePoint Designer 2010 sports a new UI, improved workflow, and improved integration between designers. Although there were doubts about the Office 2007 ribbon-style interface when it was first released, Microsoft has been steadily putting the ribbon UI in many of its products, including SharePoint 2010. The new designer also has a tabbed interface and provides breadcrumb navigation.

InstantDoc ID 103273

MICHAEL OTEY (motey@windowsitpro.com) is technical director for *Windows IT Pro* and *SQL Server Magazine* and author of *Microsoft SQL Server 2008 New Features* (Osborne/McGraw-Hill).

1&1 Web Hosting

SUCCESSFUL

"Our company was in need of high quality, yet affordable hosting for our website when we came across 1&1. For an affordable rate, we receive excellent hosting service, many powerful features and tools, and excellent customer service. One of the best features is 1&1 WebStatistics, which provides statistical feedback to our Marketing Department to track the effect that our marketing efforts have on our website traffic."

Tyler Sand, Summit Group Software, www.summitgroupsoftware.com

Visit our website for a full list of this month's special offers.

*Offers begin January 1, 2010. "6 Months Free" offer valid with a 12 month minimum contract term only. Setup fee and other terms and conditions may apply. Visit www.1and1.com for full promotional offer details. Program and pricing specifications and availability subject to change without notice. 1&1 and the 1&1 logo are trademarks of 1&1 Internet AG, all other trademarks are the property of their respective owners.

MEMBER OF united internet

Call **1-877-GO-1AND1**

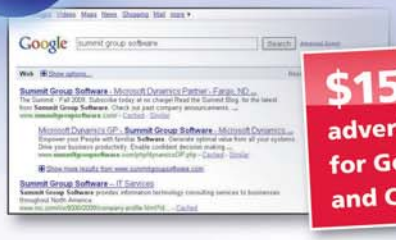
WEBSITES

start with a great web host!

At 1&1, your online success is our business. That's why we include top-of-the-line marketing features without the large price tags. Included in your 1&1 package:

Search Engine Marketing

Reach people who are looking for the products and services that you offer.



$150 in search advertising credits for Google™, Yahoo!®, and Citysearch®.

E-mail Marketing Tool

Connect with your website visitors and customers by sending marketing newsletters.

RSS Feed

Send immediate updates about special offers and news at your business.

Customer Feedback Tool

Build a positive online reputation and let your customers do the selling for you.

1&1® BUSINESS PACKAGE

Everything you need for a successful website:

- 3 Domains
- 250 GB Web Space
- 1&1 WebsiteBuilder
- Private Domain Registration
- 1&1 WebStatistics
- 25 FTP Accounts
- 50 MySQL Databases
- 24/7 Toll-Free Support

6 months FREE!*

~~$9.99~~ per month

1&1® PROFESSIONAL ESHOP

Start selling your products online:

- Easy Setup
- Traffic-boosting Tools
- Advanced eBay® Features
- UNLIMITED Website Traffic

6 months FREE!*

~~$24.99~~ per month

eBay compatible application

PayPal

1&1®

Visit us now **www.1and1.com**

Morales

"Use xbootmgr.exe to get a bird's-eye view of how your system performs during the shutdown process."

Diagnose Shutdown Problems with Xbootmgr

Use the Windows Performance Toolkit xbootmgr.exe tool to trace the source of system shutdown issues

As an IT administrator, you've probably faced an issue where one particular system will not restart in a timely fashion. Perhaps you've just updated your servers with the latest security updates, and one server has not restarted yet. This is a common issue that can be diagnosed in a number of ways, such as using msconfig.exe to turn off all nonessential services in an effort to determine which service or driver is not responding in a timely fashion. But there should be some way to get an overall, easy-to-interpret view of the shutdown statistics, to help you get a bird's-eye view of how your system performs during the shutdown process.

Enter the Windows Performance Toolkit xbootmgr.exe tool, which is supported on Windows 7, Windows Vista, Windows Server 2008, and Server 2008 R2. You can use xbootmgr.exe to generate a report that provides you with valuable shutdown information in an easy-to-interpret XML file—information that you can use to help in diagnosing your next shutdown problem. You can obtain the latest Windows Performance Toolkit by downloading the SDK for Windows 7 at www.microsoft.com/downloads/details.aspx?FamilyID=c17ba869-9671-4330-a63e-1fd44e0e2505&displaylang=en.

You do not have to download the entire SDK, however. You'll need only the actual WPT.exe files from this large download. To make the download faster, I recommend you perform the following steps:

1. On the Microsoft Windows SDK for Windows 7 and .NET Framework 3.5 SP1 page, click the Download button, then click Run in the dialog box.
2. Click Next to the resulting dialog box, then click *I agree* to the license agreement.
3. Continue to click Next until you get to the Installation Options page. Here you want to uncheck all the options except for Win32 Development Tools.
4. Click Next to begin installation. The installation will take a few seconds or longer, depending on your Internet connection.
5. After setup is finished, you will find three files called wpt_ia64.msi, wpt_x64.msi, and wpt_x86.msi in the C:\Program Files\Microsoft SDKs\Windows\v7.0\Bin directory.

Performing a Shutdown Trace

Once you've downloaded the WPT binaries, you can install the one that is the appropriate platform for your system. After Xperf is installed, you can now open a command prompt and navigate to the install directory, which by default is C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Microsoft Windows Performance Toolkit. Now type the following command to produce a shutdown trace:

```
C:\xperf\>xbootmgr.exe -trace shutdown -traceflags
   latency+dispatcher -numruns 1 -stackwalk Profile+CSwitch
```

(Type the command on one line.) Here are the descriptions for each parameter:

- -trace shutdown: Perform a shutdown trace.
- -traceflags latency+dispatcher: Enable traceflags in the latency Kernel group, plus the dispatcher Kernel flag. You can also issue the command xperf -help providers to view definitions of the trace flags.
- -numruns 1: Set the number of Shutdown runs to 1.
- -stackwalk Profile+CSwitch: Enables stackwalking for Profile and CSwitch. This switch is available only on Windows Vista and later.

Xbootmgr will perform one initial boot after which you'll need to log back onto your system. However, Xperf will perform one additional boot for each shutdown trace specified in the numruns switch. After the second boot when the tracing is finished, the Xbootmgr status window will disappear. In the previous command example, my machine rebooted twice.

After the second reboot, Xperf will automatically merge two files into one. You will need to give Xperf a few moments to merge the .etl files with the "premerge" filename into a single file. A few moments after the final reboot, you'll notice a single file called shutdown_latency+dispatcher_1.etl file in the xperf directory. Now you can export this .etl file into a shutdown XML report by issuing the following command (type on one line):

```
C:\xperf>xperf -i shutdown_
     latency+dispatcher_1.etl
   -o shutdown_demo1.xml -a shutdown
```

Viewing and Interpreting the Trace

Your next step is to open the shutdown_demo1.xml file in a browser. When you open the XML file, shown in Figure 1 and Figure 2 the first thing you should notice is that the output is formatted to have a node/leaf relationship, so that you can

Learning Path

More Windows troubleshooting articles in this series:

"Administrators' Intro to Debugging," InstantDoc ID 101818

"Bit Flips: Was That a Zero or a One?" InstantDoc ID 103154

"Conquer Desktop Heap Problems," InstantDoc ID 101701

"Disk2vhd: The Windows Troubleshooter's New Best Friend," InstantDoc ID 102980

"Examining Xperf," InstantDoc ID 102054

"Find the Binary File for Any WMI Class," InstantDoc ID 102615

"Further Adventures in Debugging," InstantDoc ID 102867

"Get a Handle on Windows Performance Analysis," InstantDoc ID 101162

"Got High-CPU Usage Problems? ProcDump 'Em!" InstantDoc ID 102479

"Reap the Power of MPS_Reports Data," InstantDoc ID 101468

"Resolve Memory Leaks Faster," InstantDoc ID 99933

"Resolve WMI Problems Quickly with WMIDiag," InstantDoc ID 100845

"Say 'Whoa!' to Runaway Processes," InstantDoc ID 100212

"Simplify Process Troubleshooting with DebugDiag," InstantDoc ID 100577

"Troubleshooting the Infamous Event ID 333 Errors," InstantDoc ID 101059

"Under the Covers with Xperf," InstantDoc ID 102263

"Disk2vhd: The Windows Troubleshooter's New Best Friend," InstantDoc ID 102980

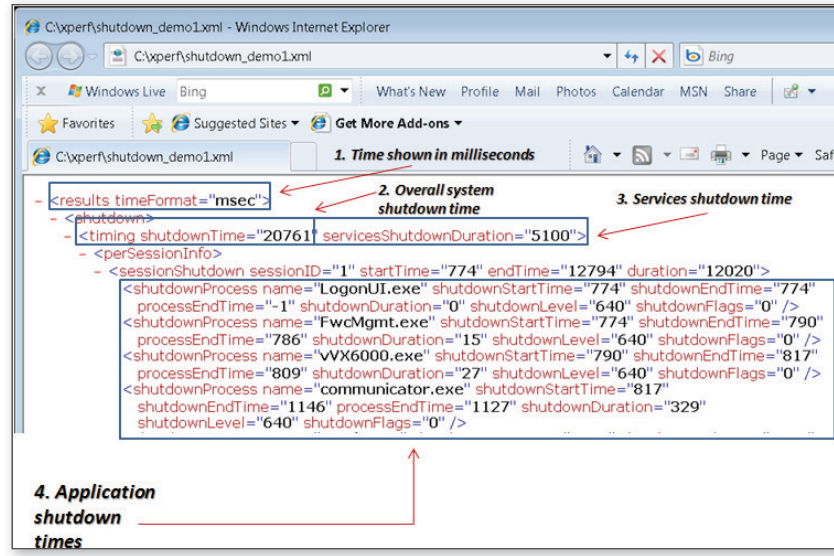


Figure 1: Shutdown_demo1.xml file, part 1

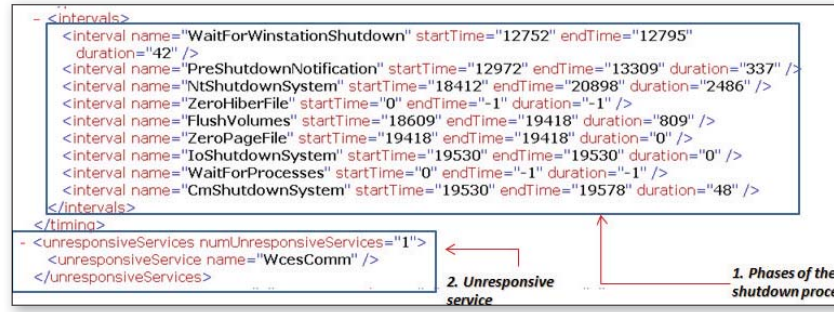


Figure 2: Shutdown_demo1.xml file, part 2

expand a single node to get more information. In Figure 1, notice some very valuable information:

- The first node shows you that the time format is in milliseconds.
- You can also see the overall shutdown time; in my example, it's 20,761ms, or 20.76 seconds to completely shut down my system.
- The services shutdown time took 5100ms, or 5.1 seconds.
- Application Shutdown listings can be found under the perSessionInfo node. This area will list the shutdown time for each application running under each session. Again, the time is in milliseconds.

Additionally, the shutdown_demo1.xml file contains the following additional pieces of useful information, shown in Figure 2.

- You can determine which services were unresponsive—that is, any service that failed to handshake correctly with the Service Control Manager (SCM). The SCM will wait 20 seconds before terminating these services, if they fail to shut down properly. In my case, I had one service, WcesComm.exe, which failed to terminate in the allotted 20 seconds.
- You can find out how long the various phases of the shutdown took to finish.

Another piece of information you might be interested in investigating is each service's shutdown details (not shown in the figures), located under the services autoStartStartTime node. Here you can find the exact length of time that each service took to shut down.

Solve Slow Shutdowns

When using xbootmgr.exe, make sure that you enter the correct syntax to collect the trace and export it to the XML report. The reason this is key is because the error handling for Xperf isn't very helpful, so you might not have a clue as to where your typo is if you make a mistake. You might find it helpful to create a batch file for these commands, so that you don't have to type them in all the time.

Become familiar with the output of the XML file. This file contains a lot of information. You can use this article as a reference to familiarize yourself with the different sections of the XML output, to help you solve your next slow shutdown issue. As always, contact me if you have any questions about this or any of my other articles. Thanks for reading!

InstantDoc ID 103315

MICHAEL MORALES (morales@microsoft.com) is a senior escalation engineer for Microsoft's Global Escalation Services team. He specializes in advanced Windows debugging and performance-related issues. For information about Windows debugging, visit blogs.msdn.com/ntdebugging.

VirtualizationPro

2010 SUMMIT & EXPO

MARCH 16-19, 2010
BELLAGIO—LAS VEGAS, NV
www.VirtualizationProSummit.com

Connect with industry experts!

Steve Riley | Mel Beckman | Michael Otey | Dan Holme | John Savill | Alan Sugano

Whether you're already working with virtualization or the technology is in your future plans, the VirtualizationPro 2010 Summit & Expo is your destination for learning everything you need to deploy, configure, secure, optimize, and manage virtualization technology.

Participate in technical in-depth sessions and workshops on:

- VDI and desktop virtualization
- Server virtualization
- Application virtualization
- Virtualized storage
- High availability and disaster recovery
- The dynamic data center
- And more!

Get the whole picture on the Microsoft Hyper-V and VMware solutions, including product comparisons

www.VirtualizationProSummit.com
800-438-6720 or 203-400-6121

- Windows XP SP3
- NTBackup
- Windows 7
- Scripting

READER TO READER

Audio Echo in XP SP3 Messaging Clients

Bret A. Bennett

One of my customers recently purchased a new Dell Vostro 1720 laptop with Windows XP preinstalled. When I had the customer use Windows Live Messenger and I connected to the Vostro over the Internet, the customer experienced a pronounced audio echo from the laptop (the video worked fine). No one else that I initiated video conferences with had this audio echo problem.

I tried replacing the motherboard, to no avail—so the problem wasn't related to a chipset defect or design issue. I also tried using a different webcam, but I experienced the same problem with a Microsoft LifeCam VX-5000 (USB webcam with built-in microphone) attached to the Vostro 1720, a Dell Inspiron 1501 laptop, and an ASUS-based desktop. Finally, I tried using a different video conferencing solution. Even with Roxio SightSpeed's echo cancellation feature enabled, the customer experienced the echo problem.

One of the most significant limitations in WSS and MOSS administration is the limited backup/restore capability

After consulting both a Dell onsite technician and a Dell Premium Support technician, I finally discovered the problem. In Windows XP Pro SP3, if you configure the microphone or speaker level through the Control Panel *Sounds and Audio Devices* applet (using the Test Hardware wizard on the Voice tab), when you get to the third step—in which you can see both the active recording and active playback meters—you'll experience progressively louder and louder echoing until you finally relent and click Cancel.

To solve the problem, start the Control Panel *Sounds and Audio Devices* applet and select the Audio tab to open XP's volume control. (The default device in the *Sound playback* section should be your internal sound chipset—it was IDT Audio on the customer's machine.) In the *Sound playback* section, click Volume. In the Master Volume box that opens, select Options and verify that Advanced Controls is enabled. Click the Advanced button, and ensure that 1 PC Speak Mute isn't enabled. (If this setting is enabled, you won't get any audio from the laptop's built-in speakers.) Make sure that neither the Master Volume slider's *Mute all* check box nor the Wave slider's *Mute* check box are enabled. Set both the Master Volume's slider and the Wave slider to about 80 percent. Close the Master Volume window.

Back on the Audio tab, click Volume in the *Sound recording* section. In the Recording Control dialog box that opens, select Options and verify that Advanced Controls is enabled. Click the Microphone slider's Advanced button, and make sure Mic Boost isn't enabled. This setting isn't enabled by default, but enabling it worsens the echo problem. Make sure that the slider's Select check box is enabled. Set the Internal Mic's slider to about 80 percent. Close the Advanced window, Recording Control window, and *Sounds and Audio Devices* applet.

Next, start Windows Live Messenger and select Tools, *Audio and Video Setup*. Run the simple wizard. Then, initiate a new video conference from your remote machine to the problematic machine. The user will immediately notice that the problem has disappeared.

Although this fix might be obvious to XP professionals, users can also benefit from the tip. I never have figured out why Windows Live Messenger's tuning wizard didn't override the faulty volume settings and provide echo-free video conferencing. I suspect that using XP's Test Hardware wizard (mentioned previously) during an XP session causes other tuning wizards to subsequently tune improperly.

—Bret A. Bennett, IT consultant

InstantDoc ID 103320

Use NTBackup to Back Up SharePoint

One of the most significant limitations in Windows SharePoint Services (WSS) and Microsoft Office SharePoint Server (MOSS) administration is the limited backup/restore capability. The existing GUI backup feature on the SharePoint Central Administration site only lets you back up or restore manually, with no scheduling support. You can create a batch file containing the STSADM command to back up SharePoint, and use Windows Scheduled Tasks to schedule the batch file—but you have to code the batch file manually. In addition, using an STSADM command lets you perform a backup only at the SharePoint site or site

Tell the IT community about the free tools you use, your solutions to problems, or the discoveries you've made. Email your contributions to r2r@windowsitpro.com.

If we print your submission, you'll get $100.

Submissions and listings are available online at www.windowsitpro.com. Enter the InstantDoc ID in the InstantDoc ID text box.

Figure 1: Configuring a new SharePoint site

collection level; you can't back up just a document library or a file in the document library.

I came up with a solution using Windows Server 2003's NTBackup utility and the shareware application NetDrive (www.netdrive.net). NetDrive is $29 per PC (free for noncommercial use); this cost is only a small fraction of a commercial SharePoint backup application.

Download NetDrive and install it on your SharePoint system. Create a new SharePoint site, and enter the appropriate information, as Figure 1 shows. The site name is any user-friendly name you want. The site IP or URL is the IP address or name of the SharePoint server. The default port is 80; change it to match your SharePoint site. The server type is WebDav. Be sure the *Connect as anonymous* check box is cleared, so you can enter the site owner's credentials. In the Account text box, enter the site owner's user name. In the Password text box, enter the site owner's password.

Jian Bo

Click Connect to establish a connection and create a map drive. (Note that if you get a WebDav unauthorized error, you need to enable basic authentication for the SharePoint site and use IIS Manager to allow WebDav web service extensions.)

Launch NTBackup from the command console, as follows:

```
ntbackup backup <sharepoint_
   mapdrive>:\docs\ /snap:off /f
   <destination>
```

Replace *sharepoint_mapdrive* with the map drive letter created in NetDrive, and replace *destination* with your desired destination backup location.

The reason for running NTBackup from the command console is to turn off Volume Shadow Copy Service (VSS), which would cause the SharePoint WebDav backup job to fail. The GUI option to accomplish this task is disabled in Windows 2003 SP1, so you must use the command line.

You can enhance the NTBackup command to include scheduling, or performing an incremental or differential backup. For more information, go to a command prompt and enter

```
ntbackup /?
```

Note that before you employ my solution, you might want to back up your network to avoid any potential data loss.

—Jian Bo, Microsoft Certified Trainer

InstantDoc ID 103321

Windows 7 on a Netbook

Everyone is excited about Windows 7, including me—but to take full advantage of the OS, I wanted to install it on

```
DISKPART> list disk

  Disk ###  Status      Size     Free     Dyn  Gpt
  --------  ----------  -------  -------  ---  ---
  Disk 0    Online       149 GB      0 B
  Disk 1    Online      7640 MB      0 B
```

Figure 2: Verifying the USB flash drive's disk number

my netbook. Because my netbook doesn't have a CD/DVD drive, my solution was to use a flash drive for installation.

To install Windows 7 on your netbook or laptop, you must first enter the BIOS and examine the boot order on your computer. Look for a USB drive or external HDD, to ensure that the computer can boot from a flash drive.

Next, you need to format your USB flash drive to make it bootable. (Note that you should use a USB drive that holds at least 2.5GB.) Open a command prompt and change your working drive to that of the USB drive (e.g., enter C:\F: to change the working drive from C to F). Enter the command

```
diskpart
```

then

```
list disk
```

to verify the disk. Figure 2 shows the output. Select the USB flash drive (e.g., disk 1). Then, enter the following commands, one at a time:

```
clean
create partition primary
select partition 1
active
format fs=fat32
assign
exit
```

Copy the contents of the Windows 7 media CD/DVD or ISO file to your flash drive. In my case, I downloaded the ISO from TechNet and used Winrar to extract the contents of the ISO to my flash drive.

Next, enter the BIOS and change the flash drive's boot priority to ensure that the drive has priority over the hard drive (and optical drive if present). Save your settings and exit the BIOS. Insert the flash drive, and boot up the machine. The installation should initiate from the flash drive. Make sure you have your CD key handy; you'll need it during installation.

—Ultan Kinahan, IT director

InstantDoc ID 103322

Ultan Kinahan

Prevent Scripts from Running on Servers

Some scripts might cause problems if you run them on specific machine types. For example, you wouldn't want domain logon scripts to run on your Terminal Server machines or other specialized systems. Although you can use Group Policy to handle this problem for logon scripts, a more general technique exists that works from within a script and lets you prevent a script from running on a particular type of machine, on a per-script basis. This solution also works for other specialized tasks.

Preventing a script from running on a specific type of machine is fairly simple if you know where to find the information about a system's domain role. The Windows Management Instrumentation (WMI) class called Win32_ComputerSystem contains a numeric DomainRole value. Table 1 lists the DomainRole values and their meanings.

Table 1: DomainRole Values and Meanings

Value	Meaning
0	Standalone workstation
1	Member workstation
2	Standalone server
3	Member server
4	Backup domain controller
5	Primary domain controller

Listing 1: OnServerQuit.vbs

```
Dim instances, instance, cs
Set instances = GetObject(_
  "winmgmts://./root/cimv2")._
  InstancesOf(_
  "Win32_ComputerSystem")

For each instance in instances
    Set cs = instance
next

If cs.DomainRole > 1 Then
    WScript.Quit
End If
```

Alex K. Angelopoulos

In general, standard logon scripts need to run only on member workstations, which have a DomainRole value of 1. You might also want to allow logon scripts to run on non-member machines that are running a workstation OS—for example, if you have home PCs that connect over a VPN and manually run a logon script to obtain resource mappings. To allow for such a case, you'd want to allow the script to run if the system has a DomainRole value of 1 or less.

The simplest solution is to use a bit of VBScript that checks the DomainRole value and quits the script if the DomainRole value is greater than 1. Listing 1 contains such a snippet of VBScript.

You can use the same technique as a safeguard for any script that you want to run only on particular platforms. For example, if you have a script that should run only on member servers but that is accessible from multiple locations or is synchronized across many machines with different roles, you can use the code with the line

```
if cs.DomainRole > 1 Then
```

changed to

```
if cs.DomainRole <> 3 Then
```

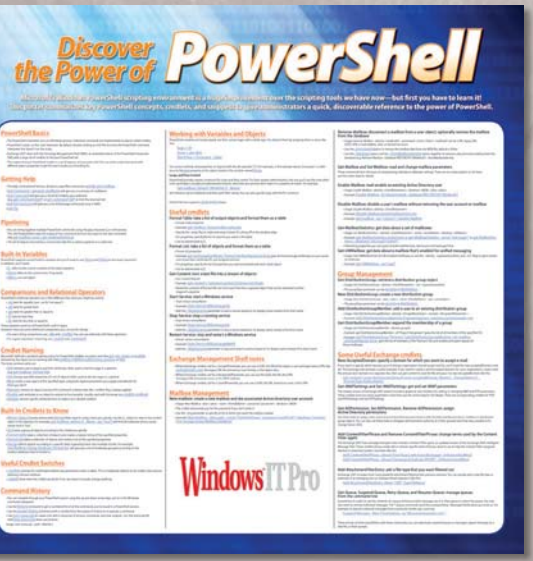
—Alex K. Angelopoulos, IT consultant

InstantDoc ID 103319

Prime Your Mind

with Resources from Left-Brain.com

Left-Brain.com is the online superstore stocked with educational, training, and career-development materials focused on meeting the needs of IT professionals like you.



Featured Product:

Windows PowerShell Poster
Discover the Power of PowerShell

Microsoft's Windows PowerShell scripting environment is a huge improvement over other scripting tools, and we can help you learn it! Our new PowerShell poster summarizes key PowerShell concepts, cmdlets, and snippets for group management, Exchange, and other admin tasks.

Topics covered are PowerShell basics, pipelining, built-in variables, mailbox management, command history, and much more!

Only $14.95*!

Order your poster and discover other great PowerShell resources now at Left-Brain.com

left-brain

*Plus shipping and applicable tax.

www.left-brain.com

Windows IT Pro

- Bitlocker
- Outlook
- Remote Desktop
- Hyper-V
- Windows 7

ANSWERS TO YOUR QUESTIONS

Q: Should I use folder redirection or roaming profiles in Remote Desktop, Virtual Desktop Infrastructure (VDI), and other environments?

A: In most scenarios, this shouldn't be a choice. Rather, you want to use both technologies, because they complement one another to achieve the optimal virtualized user state environment. It's critical to use both any case where users may use multiple OS instances, such as people who use multiple computers, users in a Remote Desktop/Terminal Services environment, or VDI infrastructure.

A normal user state consists of the user's data, such as information in the Documents or My Documents folders, and the user's settings, which include personalization and configuration. User settings mostly live in the registry, and the user portion of the registry is stored in the user's ntuser.dat file.

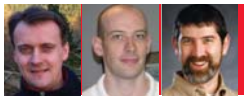
Normally, this user state, called a local profile, is stored in a subfolder of C:\Users (in Windows Vista and above) and is local to each machine. When your network is configured to use local profiles and a user logs on to different physical machines or connects to different Remote Desktop services or VDI instances, the user will have different data and different settings on each OS instance, because the user has a different local profile on each instance. This is undesirable for the end user.

The solution is to abstract the user's state from the OS instance, which enables the user state to follow the user no matter which OS instance the user is using. This abstraction is where folder redirection and roaming profiles are used. Roaming profiles is a technology in Windows that replicates the local profile to a network location. No matter which OS instance a user logs onto, the same profile is always used.

Traditionally, roaming profiles worked by replicating the profile from the network location to the local machine during logon then replicating it back up to the network location when the user logs off. This profile replication delays a user's logons to an OS instance because the profile data has to be copied from the network. It also delays logoff, because the profile has to be replicated back to the network. Obviously, the more data in the profile that's changed, the longer the replication takes.

Each version of Windows has made improvements to the replication mechanism, and with Windows 7 there are two notable changes. One is that only the changes to files are replicated, not entire files. The other is that you can configure ntuser.dat to replicate in the background during a session, eliminating the slow logoff because of the state information has already been replicated to the network. This second feature isn't enabled by default—you need to enable this background synchronization using Group Policy.

Roaming profiles still has to replicate the information in the profile back and forth between the user's OS instance and the network. As the amount of user data, such as the content of the Documents folder, grows, it can add up to a lot of data requiring synchronization. This is where folder redirection is used. Folder redirection allows you to change where the folders that make up the user profile point. Instead of the folders being part of the user's profile area, they can be folders on a network location. These folders include application data (AppData/Roaming), Desktop, Documents, Pictures, and the Start menu. Windows Vista and above, you can also redirect Contacts, Downloads, Favorites, Links, Music, Saved Games, Searches and Videos. You can see that basically every location where data is stored for a user profile can be redirected to another location, allowing you to take all the data elements of the user's state and remove them from the profile. This means a much smaller roaming profile and so less to replicate. Additionally, folder redirection



Jan De Clercq | jan.declercq@hp.com
John Savill | jsavill@windowsitpro.com
William Lefkovics | william@mojavemediagroup.com

Q: How do I enable background uploading of the user state of a roaming profile in Windows 7?

A: Windows 7 and Windows 2008 R2 introduce the ability to have user settings synchronize in the background during a user's session instead of waiting until the user logs out. This means at logoff there is less information to replicate, which gives you a faster logoff. You enable this setting using group policy by navigating to Computer Configuration, Administrative Templates, System, User Profiles, and double-clicking Background upload of a roaming user profile's registry file while users is logged on. Set this option to Enabled and set the scheduling you want to use—either based on a time interval or at set times of day.

—John Savill
InstantDoc ID 103155

means user data is on a network store, so backup for your organization is easier.

Even though a user's data may be redirected to a network location via folder redirection, the data is still available if the user is offline from the network thanks to the offline files technology in the OS. Offline files, which is enabled by default, caches data on the user's local machine in a client side cache. Windows 7 improves the background synchronization of offline files by automatically synchronizing changes without a user selecting if they're online or offline. Windows 7 also introduces transparent caching, which automatically caches files locally on the client when they're downloaded from a network location. This transparent cache means that if a user views a remote file, closes the file, then opens it again, the second read would be fulfilled from the users transparent cache. This feature results in a much faster read experience. Note that transparent caching still contacts the server to ensure the local cache is current, so data in the transparent cache isn't available offline and isn't a replacement for offline files and folders.

To achieve the optimal roaming user experience, you need to use roaming profiles, offline folders, and folder redirection. You might also look at Microsoft Application Virtualization (App-V), a technology that facilitates very fast application delivery to OS instances. With App-V, in addition to the users' states following them no matter which OS instance they use, their applications can also follow them.

—John Savill

InstantDoc ID 103150

Q: Can a Hyper-V guest use pass-through disks and still use Live Migration?

A: Live Migration is the technology that copies the memory of a running Hyper-V guest to a target node while the guest is still running, which means there's no downtime of the guest required to transfer the virtual machine (VM) state from one Hyper-V host to another. To solve the time delay of dismounting and mounting the LUN that holds a VM's VHD files, the system uses Cluster Shared Volumes (CSVs), which allows all nodes in the cluster to access the CSV enabled storage concurrently, so no dismount/mount operation is needed.

If you're using pass-through disks, your pass-through disk can't be part of the CSV namespace, because the Hyper-V host isn't actually mounting the storage. The guest performs I/O directly, which means the storage isn't accessible to all nodes at the same time. In the Failover Clustering configuration of the VM, you'll configure the pass-through disk as a dependency for the resource group, so when you perform a Live Migration the pass-through storage will have to dismount from the current Hyper-V host and mount on the new Hyper-V host. This process will slow down the migration of the VM and probably cause a noticeable pause to clients, or even disconnects.

The answer is, then, that you can still use Live Migration with pass-through disks, but the dismount/mount of the pass-through will take time and may break the TCP connection timeout. Your best option is to use VHDs instead of pass-through, because VHDs can be part of CSVs, and you won't need the dismount/mount operation. VHD and pass-through disk performance is basically equal, so performance isn't a major concern.

—John Savill

InstantDoc ID 103123

Q: When I try to install Outlook 2007 Business Contact Manager on Windows 7, I get an error message. What's wrong?

A: Outlook 2007 Business Contact Manager (BCM) uses SQL Server 2005 Express as the database for the Customer Relationship Management (CRM) application. All editions of SQL Server 2005 have compatibility problems with Windows 7. These problems have been addressed in SQL Server 2005 Service Pack 3 (SP3).

When you install Outlook 2007 BCM on a workstation running Windows 7, you'll see a compatibility warning. If you click the Check for Solutions Online button, the current outcome returned explains that there is no solution available. You can continue the installation by selecting the Run Program button. After you've completed the installation of Outlook 2007 BCM, don't start Outlook. Download and install SP3 for SQL Server 2005 Express first—you can download it from Microsoft.

Outlook 2007 BCM will install SQL Server 2005 Express by default as part of its installation process, but if a previous installation of SQL Server 2005 exists, you'll have the option of using it to host the BCM database. This means that you could install SQL Server 2005 Express and apply SQL Server 2005 SP3 even before you install Outlook 2007 BCM.

Whether you install SQL Server 2005 separately or as part of the Outlook 2007 BCM installation, you need to apply SQL Server 2005 SP3 prior to running Outlook 2007. Outlook 2007 BCM will then function as it's expected to on Windows 7. Of course, you should update Outlook with the latest Office service packs and patches with Microsoft Update or your enterprise patch management solution.

—William Lefkovics

InstantDoc ID 103015

Q: What type of disk configurations does BitLocker Drive Encryption (BDE) support? Can I use BDE on iSCSI or Fibre Channel drives? Is anything different from older OSs in Windows 7 and Windows Server 2008 R2?

A: In Windows 7 and Server 2008 R2, you can use BDE on USB, FireWire, SATA, SAS, ATA, IDE, and SCSI drives. At this point, you can't use BDE on iSCSI, Fibre Channel, eSATA, or Bluetooth drives. Compared to the initial BDE release that's included in Windows Vista and Server 2008, the Windows 7 and Server 2008 R2 BDE release adds support for BDE encryption on removable storage devices such as portable hard drives and USB flash drives. This addition is possible thanks to the new BitLocker To Go (BTG) extension.

Note that BDE isn't available in all Windows 7 versions. As in Vista, BDE is included only in the Windows 7 Enterprise and Ultimate editions—the versions that target high-end home and business users. BitLocker support is included in all Windows Server 2008 and Windows Server 2008 R2 editions.

—Jan De Clercq

InstantDoc ID 103171

What's New in Windows Server 2008 R2

Bill Laing discusses new server roles and how IT pros can maximize their software investment

by Michele Crockett and Michael Otey

Bill Laing, corporate vice president of Microsoft's Windows Server Division, recently sat down with Michael Otey, technical director of *Windows IT Pro*, and Michele Crockett, editorial director, to discuss the release of Windows Server 2008 R2. As Laing pointed out, this is the first server release to be timed with a client release—Windows 7. Laing talked about the scenario-focused development process that produced both products and the tight integration with third-party partners. Although Server 2008 R2 doesn't lack for cool new features, its most riveting qualities—such as Core Parking—are those that save resources, time, and aggravation for IT pros. Here Laing tells how listening closely to customers and partners yielded a product that helps businesses operate more efficiently in a tight economy.

Michele Crockett: What have you heard from the launch events that people are most interested in and excited about?

Bill Laing: I think the big-ticket item is our virtualization. We had a great reception to V1 of Hyper-V, but there were some other things we needed to do, particularly add Live Migration and cluster support. And when I think of this server, I think of two things. I broadly think of the attributes of the basic system: the core system. But I also think about it by workload—the file server workload, the Active Directory, file and print, web server—and I think of these as separate. Each workload offers some exciting things.

For example, Active Directory has the Recycle Bin, which seems like a fairly small feature. But when you talk about it, you get spontaneous applause. When we were planning the release, we did a number of things to get input from different people. I split feedback into three categories: the voice of the customer, our business people, and the technology. We asked ourselves, "Is this the voice of the customer, the business, or the technology?" Moving into 64 bits or virtualization are technology drivers, and then you might turn it into some customer need as well.

I use what we call red zones. Every quarter we take all the calls into our support center (CSS)—they catalogue every call—how long it took and what area it was. I have them roll those up and give me [what topics received] the most calls, the longest ones, and I use that to prioritize things. And the calls aren't always about a system crash. One of the highest-level calls, from my point of view, was from customers who had deleted accounts accidently from the domain controller, or they had corruption and didn't have a backup. That was one of the things that drove [development of the AD Recycle Bin].

Michele Crockett: Are you getting a feel from people about adoption and how quickly they might move to Server 2008 R2?

Bill Laing: It does seem to be a little faster than Server 2008. I'm not quite sure why. I think they got used to 2008, and Server 2008 R2 feels less disruptive to them. We try to do that with an R2 release.

Michele Crockett: And some companies are probably moving from Windows Server 2003.

Photograph by Jim Molnar

Bill Laing: Yes. As you get close to the end of the support cycle, people start to think about 2003 and upgrade plans. Virtualization also gives them a bridge to the past if they want because they can move to that and still run old programs. And there's a lot of pressure on cost and power. A couple of customers I've talked to, just by consolidating the number of machines and running in VMs, have gone from 15 machines to 3. Forget any fancy software we did on power saving—they're running 3 machines instead of 15!

Michele Crockett: Our readers talk about working with limited budgets. They ask what they should do first, what things really need to go together. Do you have any insight into that topic for the IT pro who doesn't have a large budget to work with?

Bill Laing: Virtualization is one of the biggest and easiest wins because you can reduce the number of machines. It's hard data to get, but if I had 50 machines and still keep 50 VMs, how much less is my management effort? It's clearly less, but it's not like running 1 machine; you still have 50 OSs to run, but there are some savings there. We did a lot of power management in the new OS, and it's pretty dramatic—it exceeded my expectation of what we would do.

Until recently, idle servers typically consumed just about as much power as when they were fully utilized. We didn't do much power management, and there wasn't a lot on the chips. But we've driven that down dramatically to 40 percent, to 50 percent power utilization when servers are idle.

Michael Otey: Core Parking is a cool feature because it's enabled automatically right out of the box. On one of the first systems I used, I opened Resource Manager and I could see that as the system is active, all the CPUs in it are active. As you stop doing things, the system automatically parks them and there's nothing you need to do to make that happen.

Bill Laing: It used to be, "Well, I have all these cores, and I'll just run my workload across them." Now you say, "What's the least number of cores I can use to get through the work?" It's the small changes like this, where people don't actually have to do anything, that get attention. We've also done a lot more work on PowerShell so people can automate a lot more.

Michael Otey: The new PowerShell Integrated Scripting Environment is really nice. That feature really helps people and administrators get started with PowerShell because it gives them a graphic, color-coded editor that makes it really easy to learn.

Michele Crockett: That's a big deal with our audience—they love PowerShell.

Bill Laing: We have a blog and a site for PowerShell, and it's one of the most popular places that people come to. People like the idea that you can take a script that someone else wrote and perhaps refine it or reuse it, so there's another big time-saving opportunity.

Michael Otey: Server 2008 R2 contains a lot of features. Can you give us some idea of the development scope? How many people worked on this and for how long?

Bill Laing: It's hard to estimate the number of people because we share the work between the client and the core. There's a core OS team, a client team, a server team—and we tend to think of it as the base system and then the workload. But some teams started probably about a two-year cycle of development. Some people started before 2008. One of the things I've tried to drive is that it's much more important to deliver complete scenarios for end users than do lots of features that you have to complete yourself, or all the pieces aren't there.

So we use a model called CMD, or customer-focused design, where we interviewed a lot of customers and partners (hardware partners are a key part of the release) and then tried to build the core things that customers told us were needed. And we very specifically wrote down everything in their words, not our words. Traditionally, we'd interview people and the employee would come back and say, "Well, what they really want is this," and that would be the thing that the person interviewing them wanted to build, not what they really wanted. So we disciplined ourselves to write down what they said, and we used that to guide us.

And the second part of that was rather than saying, "We'll ship when we have less than X number of bugs" (which would be a traditional way of doing it), we used guidelines called CTQs (credible to quality). So we might say we can support X many users in a VDI session doing this, or something around the speed of Live Migration will be this speed, rather than saying Live Migration ran and didn't crash in 24 hours. Every team had CTQs that we'd hold them to, which is a different model than we've used in the past.

We also have a lot of telemetry in the system, so we can measure the roles people have installed. People can opt in to provide data anonymously, and our beta site customers (we call them our TAP customers) actually enter additional information. TAP is our Technology Adoption Program for customers who would take the airway release and give us feedback. There used to be people whose job it was to call them every week or two weeks and say, "How many servers have you deployed? I have to report back to my boss." Now they're automatically enrolled and we get the telemetry. We can tell them, "By the way, you're actually running 53 web servers." And they'd say, "Wow, we didn't know that." We measure what roles are installed, which tells us the coverage we got during testing. In the past, you really just had to hope sometimes that you put the beta out. So I feel really good that we've got a good rhythm going with customers. We've built up that level of trust.

Michele Crockett: I think IT pros might still be used to waiting for the R2 version, even though I know Microsoft has tried to change the release rhythm. Do you think you've made any headway with people not waiting for R2?

Bill Laing: I think it takes a long time to rebuild that belief in you, and I feel like we've had a really good track record from 2003 onward—relatively predictable release seasons, good time frame, not waiting for the first service pack to come, so I think people are more comfortable with that.

We also work closely with our hardware vendors to make sure that they are systems-ready at the release. Sometimes that's their main interest, sometimes they have core features that they want to work on with us before the release. Typically, Intel, AMD, and

Windows IT Pro

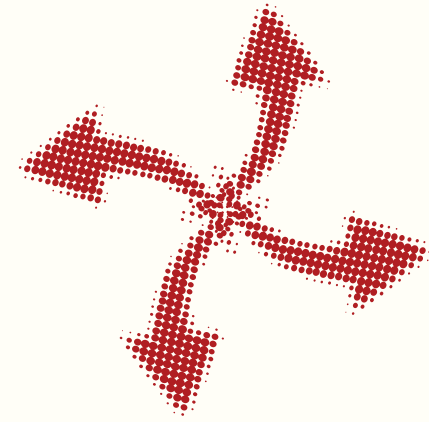
Exchange 2010:
The Future of Messaging

Build your unified communications future on a strong Exchange Server 2010 foundation

What does the future of messaging hold? Exchange Server MVP Paul Robichaux spells it out in this series of three articles. You'll learn about:

- The performance and storage-related changes in Exchange 2010, including changes to the physical layout of the database, replication performance improvements, and the new database availability group (DAG) feature for mailbox replication, high availability, and disaster recovery.
- New client-oriented features, including an all-new version of Outlook Web Access that supports Safari and Firefox, productivity improvements like MailTips and conversation view, and new features for mobile device users.
- The technical foundation for hybrid Exchange 2010 deployments and the basics you need to get started using them.

Read on to learn about these new features and to understand how Exchange Server 2010 provides a strong foundation for building Unified Communications.



by Paul Robichaux

"The reason you can't use Transporter Suite to go directly from Domino to Exchange 2010 is that Microsoft didn't update the tool for Exchange 2010."

- InfoWorld.com (Oct. 21, 2009)

"Microsoft recently said that it will not support the tools (the Microsoft Transporter Suite) for Exchange Server 2010 because there are better third-party options."

- SearchExchange.com (Nov. 19, 2009)

"There is no Transporter Suite in Exchange 2010 - it has been dropped."

- MSExchange.org (Dec. 1, 2009)

"Certainly the Transporter Suite is critical if you want to have Interorg free/busy calendar information."

- TechTrooper.net (Dec. 17, 2009)

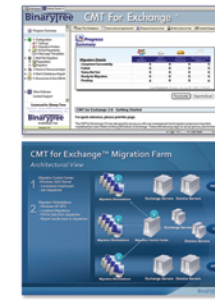
Introducing the only software to establish direct interoperability and a direct migration path between Lotus Domino and Microsoft Exchange Server 2010.

Establish Platform Interoperability with CMT for Coexistence™ 3.0

Whether your organization needs to migrate over an extended period of time or needs to coexist long-term with both platforms, CMT for Coexistence 3.0 establishes robust interoperability with directory synchronization, calendar free/busy lookups and more, between Domino and Exchange 2010.

Migrate to Exchange Server 2010 with CMT for Exchange™ 3.1

CMT for Exchange 3.1 migrates the email, calendars, contacts, tasks, attachments, and more of Lotus Notes users from Lotus Domino to Microsoft Exchange Server 2010 with unmatched data fidelity, migration management capabilities, and throughput.



No complex, two-step migrations. No long delays. Our software is recommended by Microsoft for their Enterprise Notes Migration Methodology and is ready for delivery today.

To learn more, review our resources on migrating to Exchange 2010 at **www.binarytree.com/Exchange2010**.

BinaryTree

www.binarytree.com | sales@binarytree.com | Worldwide: +1-212-244-3635 | In the U.K.: +44 (0) 20 7692 5661 | In Germany: +49 69 66 55 43 79

EXCHANGE 2010 RESOURCES

BinaryTree

www.binarytree.com/Exchange2010

SOLUTION:

Binary Tree offers the CMT suite of software for migrating users from Lotus Domino to Microsoft Exchange Server 2010 and Exchange Online. CMT Inspector™ analyzes Notes mailboxes so you can properly plan your migration. CMT for Coexistence™ establishes directory synchronization, calendar free/busy lookups, and high-fidelity interoperability between Domino and Exchange 2010. CMT for Exchange™ offers unmatched migration management, data fidelity and throughput for migrating mailboxes from Domino to Exchange 2010. The CMT software suite also contains solutions for analyzing Notes applications, migrating Notes applications to SharePoint, and for consolidating and retiring Domino after a migration.

Microsoft®

www.microsoft.com/exchange

SOLUTION:

Now, more than ever, your organization requires cost-effective and flexible communication tools. With Microsoft Exchange Server 2010 you can achieve new levels of reliability and performance with features that simplify your administration, help protect your communications, and delight your users by meeting their demands for greater mobility. Microsoft Exchange Server, the cornerstone of Microsoft's Unified Communications solution, is a flexible and reliable messaging platform that can help you lower your messaging costs by 50 percent to 80 percent, increase productivity with anywhere access to business communications, and safeguard your business with protection and compliance capabilities that help you manage risk.

CONTENTS

Exchange 2010 Anywhere Access
page 4

Exchange 2010 Goes Hybrid
page 7

Exchange 2010 Storage and Performance Improvements
page 9

Paul Robichaux is a senior contributing editor for *Windows IT Pro* and a Microsoft Exchange MVP and MCSE who specializes in helping people understand how to get the most from Exchange. Paul's most recent book is the *Exchange Server Cookbook* (O'Reilly and Associates) and he blogs at www.robichaux.net/blog <http://www.robichaux.net/blog> .

Exchange 2010 Anywhere Access

By Paul Robichaux

Exchange 2010 continues Microsoft's theme of offering "anywhere access." Of course, "anywhere" is a pretty broad location, so in fairness I should note that none of the features I describe in this article will work if you are on the Moon, at the bottom of the Marianas Trench, or anyplace else from which you cannot get an Internet connection. Even with that restriction in mind, though, plenty of improvements in Exchange 2010 and its companion products make life better for mobile users.

For our purposes, we can assume that "mobile" includes three overlapping groups of users:

- Travelers using Outlook on portable computers
- People using mobile devices that support Exchange ActiveSync
- People who access their mailboxes with Outlook Web Access

Each of these constituencies get some goodies with the new Exchange release. As a bonus, so do Exchange administrators. Let's take a look.

The New Outlook Experience

Take a look at the screen shot in Figure 1 and you'll notice a number of new features in Outlook 2010. The Office fluent interface (which most of us just call "the ribbon") has been expanded and reorganized, with a major chunk of space dedicated to the new Quick Steps toolbar, which allows you to quickly set up one-click actions to move, flag, and otherwise manipulate items. You can create Quick Step actions to create new items, forward existing ones, mark tasks as complete, and so forth. The actions you create here are stored in the hidden "Quick Steps Settings" folder that Outlook 2010 creates in your mailbox. This allows your definitions to be portable between different machines, and opens the eventual possibility that Quick Steps will migrate to OWA too.

Another major change is the content of the Delete tab on the main Outlook ribbon. This tab contains two important, and useful, Outlook 2010-only features: the Ignore button and the Clean Up command. Ignore is one of my

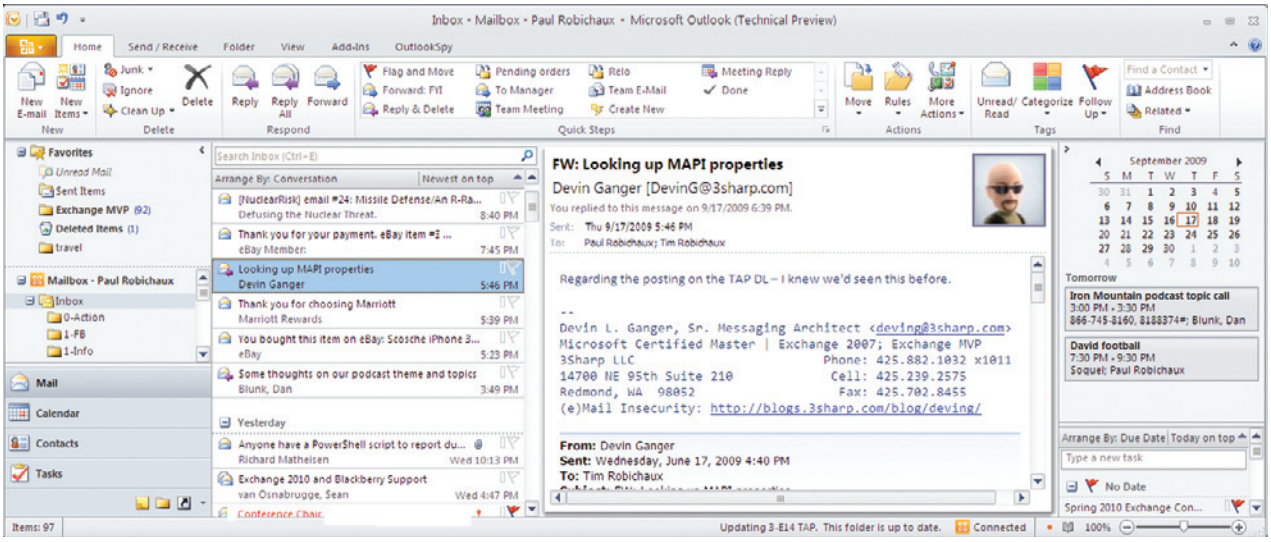


Figure 1: Outlook 2010

favorite Exchange/Outlook 2010 features; when you click it, Outlook silently creates a new rule in a special hidden folder (the Conversation Action Settings folder) that will move any further messages in the same thread to the Deleted Items folder. Think of it like a mute button for long-winded threads. The Clean Up command does something similar by walking through all the messages in a single conversation and deleting any early messages whose text is already contained in a later reply or forward.

You're probably already familiar with the new Conversation view in Outlook 2010; it displays messages in a thread in the reading pane, including your replies, forwards, and messages that have been stored in other folders. It's quite different from the conversation view in Outlook 2007 and earlier, and it takes some getting used to. However, once you understand how to use it, it's quite valuable.

All of these features are enabled by the fact that Exchange 2010 creates and maintains its own conversation threading data, taking into account not just the subject header but other message properties that help it keep track of conversations even if the subject is changed midstream. The conversation metadata is generated when the message arrives, so it will only be present (and thus used by Outlook) for messages that have arrived at and been processed by an Exchange 2010 Hub Transport server.

Outlook 2010 sports another feature that's guaranteed to be a huge favorite with a certain class of people: the ability to maintain multiple MAPI accounts in the same profile. This is incredibly valuable if you have both work and home Exchange accounts (as I suspect many of you do), or if you need to simultaneously access a work account and a second account on a customer's server. Outlook integrates multiple accounts very smoothly, showing them as separate nodes on the folder tree and allowing you to easily see side-by-side calendars.

OWA Grows Up

The component formerly known as Outlook

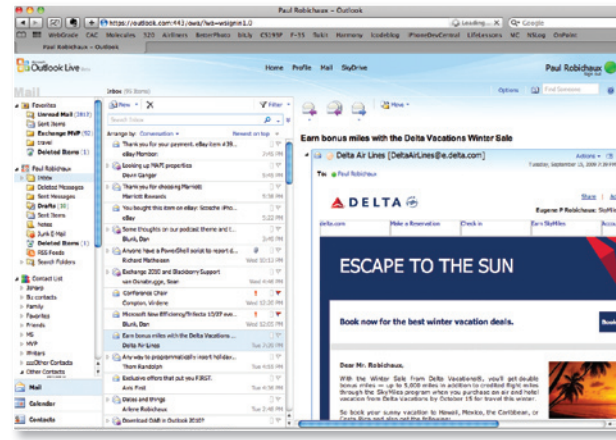


Figure 2: Outlook Web Access 2010 running on Mac OS X's Safari browser

Web Access has a new name: Outlook Web App. It wouldn't have been a bad idea for Microsoft to come up with a completely new name because OWA itself is almost brand-new. There are too many features in the new OWA for me to list here, but a few of the highlights are worth mentioning because they put the "access" in "anywhere access."

First, the premium mode of OWA is supported in two additional browsers: Safari (Mac OS X only) and Firefox 3.x (Linux, Mac OS X, and Windows). If you're accustomed to getting the OWA Light experience when using one of these browsers, you'll probably be pleased with the new OWA's feature parity. Figure 2 shows a view of my mailbox from OWA 2010 in Safari on Mac OS X; Figure 3 shows the same mailbox in IE

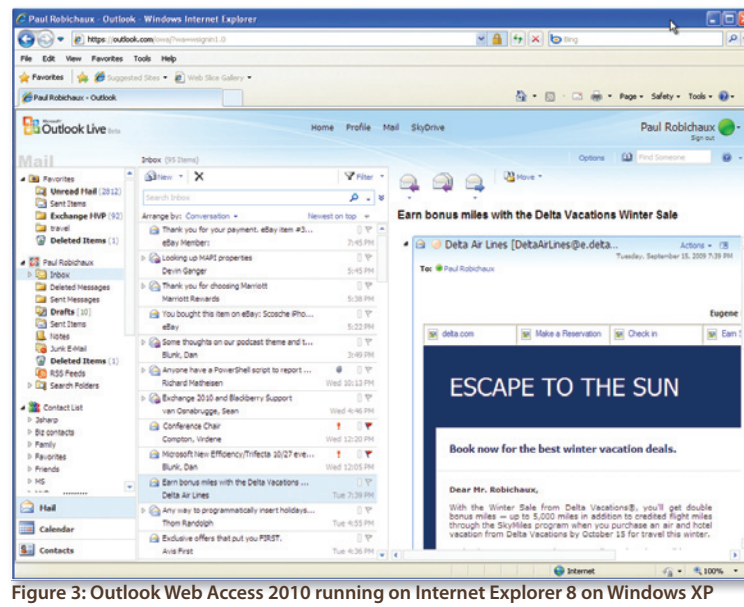


Figure 3: Outlook Web Access 2010 running on Internet Explorer 8 on Windows XP

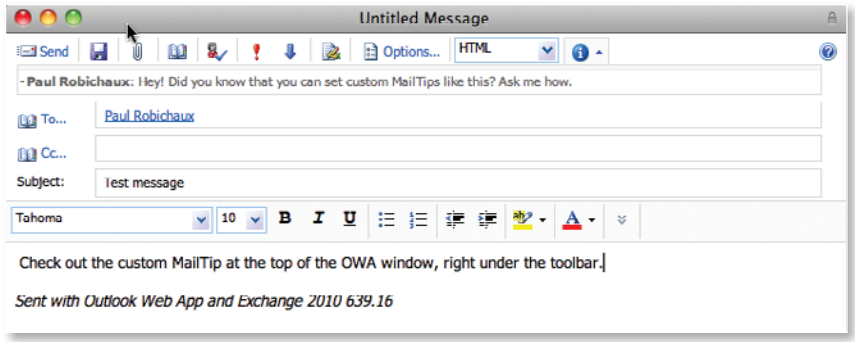


Figure 4: A custom MailTip

8.0 on Windows XP. As you can see, there's little difference in visual appearance between the two: both have integrated instant messaging, search, and all the other nifty new OWA 2010 features (like the ability to just scroll through a folder without having to page through it).

Second, Microsoft has put a lot of effort into insuring a consistent experience between OWA 2010 and Outlook 2010. Personal Archive access is a great example. If your mailbox has a Personal Archive associated with it, the archive mailbox shows up in OWA and Outlook and behaves identically in both places. You can drag messages between your archive and other mailbox folders.

MailTips are another example: these custom alerts give the sender of a message useful information before the message is sent. For example, if you try to send a message to someone who's got their out-of-office message turned on, you'll see a MailTip telling you so. Thus forewarned, you might decide not to send the message if the recipient won't be able to act on it immediately. Built-in MailTips exist for a number of other circumstances, including sending messages to external recipients, sending to large distribution lists, sending to moderated distribution lists, and so on. A new Exchange service called the Exchange Group Metrics service gathers information on DL membership that can be used to intelligently display MailTips. Other data items are retrieved directly by, and cached on, the client. You can also define your own custom MailTips, as shown in Figure 4.

Custom MailTips are set on a per-mailbox basis using the –MailTip switch for the Set-Mailbox cmdlet, like this:

```
Set-mailbox paul@robichaux.net
-MailTip "Help! I'm trapped in the server
room. Please let me out!"
```

You can also control which types of MailTips are available throughout your organization with the Set-OrganizationConfig cmdlet.

There's more, too: Outlook, OWA, and Outlook Mobile now share the nickname cache that used to be solely for Outlook, meaning that your suggested contacts will follow you from platform to platform. You'll find many other examples of this feature across the three products, not the least of which is Conversation view.

Mobility

The big news from a mobility standpoint is the release of a new version of Outlook Mobile, Outlook Mobile 6.5. In the past, almost the only way to get a new version of Outlook Mobile was to buy a new device. However, for Exchange 2010 Microsoft has unbundled Outlook Mobile and packaged it as a separate download through a clever multi-stage mechanism. Exchange 2010 users can visit a link that points to the Exchange CAS server that will download a small bootstrap loader to their Windows Mobile 6.x device. The bootstrap loader in turn will download the correct release of Outlook Mobile for the device they have. Once installed, the new version supplants the built-in version. This is a welcome change from the status quo, because Windows Mobile devices are generally not upgradable in the field.

The new version implements the same Conversation view that Outlook 2010 and OWA 2010 have, while still retaining the useful shortcuts and key commands from older versions of Outlook Mobile. If you like, you can enable sync of SMS messages from the phone to your Inbox, and vice versa; with this feature turned on, SMS messages appear alongside email messages and OCS conversation and call notifications. Because all these disparate data types are in one place—your Inbox—you can filter, sort, search, and organize them together despite the fact that they originated in different locations.

Delivering anywhere access was one of the key pillars of Microsoft's strategy for Exchange 2010. While it's clearly too early to see how these features will be adopted in the marketplace, they certainly offer a great deal of potential. Having the same consistent interface and feature set across multiple clients is a big win for end users, and the array of "anywhere access" features that Microsoft is delivering in the Exchange/Outlook 2010 wave will help drive broader adoption of both products.

Exchange 2010 Goes Hybrid

By Paul Robichaux

Software as a service (SaaS) is a growing part of the IT market. Precise estimates vary widely according to the analyst firm you ask, but there's no doubt that cloud-based service offerings are taking an increasing chunk of both mindshare and budget. Not wanting to miss out on anything, Microsoft has its own line of service offerings that it collectively refers to as Software + Services (S+S). Microsoft's S+S model places a heavy emphasis on smooth integration between Microsoft-hosted services and servers running on customer premises (known as "on-premises" or just "on-prem"). Microsoft's claim is that this gives customers the greatest degree of choice by letting them decide what to run themselves and what to let Microsoft host.

Exchange 2010 changes

Exchange 2010 has been touted as the first version of Exchange designed to be run as a service or on-premises. Previous versions of Exchange have been hosted by companies large and small, but these hosted offerings required a lot of behind-the-scenes work from the hosting providers, as well as Microsoft tools like the Hosted Messaging and Collaboration (HMC) toolkit.

Microsoft made a number of architectural changes in Exchange 2010 to make it better suited to hosting environments. As a happy side effect, many (but not all) of these changes also improve its utility or performance for people who are running it on-premises. Here's a summary of the most important changes from a hybrid perspective:

- Databases are now fully independent of the server they live on; in fact, they're independent of the Exchange organization in which they are created. This makes it much easier to move databases between servers.
- A mailbox can be moved between databases even while its owner is logged on to it, essentially eliminating move-related downtime. Moves can be scheduled and queued with much more flexibility than in Exchange 2007.
- Remote PowerShell provides the full power of the Exchange Management Shell across machines (and Active Directory forests). Because the Exchange Management Console (EMC) is based on this functionality, it gains the ability to connect to multiple Exchange organizations and manage them, no matter what Active Directory forest you're in.
- Role-based access control (RBAC) allows you to set permissions not only on individual EMS cmdlets but even on the arguments passed to them. You have very fine-grained control over which users may use which commands and which arguments, making it much easier to restrict what hosted service administrators can do.
- The Exchange Control Panel (ECP) provides more self-service control for users, including the ability to create and manage distribution lists. Of equal importance, with the ECP you can access some Exchange administrative features even without the Exchange Management Console (EMC).

These new features raise some extremely interesting possibilities, including mailbox moves using the standard Exchange tools (which means being able to perform online moves and to schedule moves) and calendar federation with outside organizations so that federated users can see each others' free/busy status.

Two Services, No Waiting

Before we can dig into the details of how to build and operate a hybrid Exchange organization, we have to define what

your organization is hybridized with. Microsoft actually offers two different hosted Exchange services:

- Live@EDU is Microsoft's overall service offering for the educational market. In addition to student mailboxes, Live@EDU deployments frequently have other Windows Live services like Live Messenger and SkyDrive, plus on-premise faculty and staff mailboxes. You may also have heard of Outlook Live; it's the mail client piece of Live@EDU, a hosted OWA environment currently based on a pre-release Exchange 2010 build.
- Exchange Online is part of Microsoft's Business Productivity Online Services (BPOS) line. It's the business equivalent of Outlook Live; BPOS also includes hosted versions of SharePoint and OCS 2007. As of this writing, Exchange Online is hosted on Exchange 2007; Microsoft will be moving BPOS users to Exchange 2010 sometime after the product RTMs.

While the core feature set of these three offerings is the same, some of the details of how they function in hybrid environments vary according to which hosted offering you're using. For the rest of this article, I'm going to focus on Exchange Online because it's the service that most Windows IT Pro readers will be likely to encounter.

The Basics of Hybrid Design

From a design standpoint, it makes sense to assume that virtually every hybrid Exchange 2010 organization will start off as an Exchange on-premises organization. This isn't a requirement; you could certainly start with hosted mailboxes and expand by adding an on-premises Exchange installation, but very few organizations do so. With that in mind, let's take a look at how you design a hybrid environment.

The first thing to design is what you're trying to accomplish: migration from your existing system or coexistence. Microsoft's hybrid "software + services" model is targeted at the latter, but some organizations may decide that they want to go all-hosted. Microsoft provides tools for both cases, of course.

The next consideration most people encounter is which mailboxes go on your servers and which will be hosted by the online component. The answer will be determined by a number of factors that I won't go into here, including whether you're using Microsoft's BPOS "deskless worker" option. You'll need to make that determination on your own based on who your users are, how many of them you have, and what mix of self-hosted and cloud-based services make the most sense for your needs.

On the migration front, Microsoft ships tools for migrating email from Exchange, POP3, and IMAP4 servers. You use these tools (known collectively as the Microsoft Online Services Migration Tools) to permanently move e-mail from its current location to mailboxes on the BPOS side. If you're currently using an IMAP4 or POP3-based system, the migration tools require you to create a CSV file containing the list of mailboxes to move, then to run a migration wizard. If you're using Exchange, you can move mailboxes from your existing Exchange organization to the new one using the Move Exchange Mailboxes to Microsoft Online Services Wizard (how's that for a product name?) The experience is much like that of moving mailboxes using the native Exchange tools, with the exception that the wizard gives you the option to keep or remove the local mailbox, and that it moves the newest messages in the mailbox first.

Setting Up Coexistence and Migration

Next, you have to design a coexistence plan if you're going to co-exist. BPOS includes the Microsoft Online Services Directory Synchronization tool (which most people just call "dirsync") can perform one-way synchronization from your organization's Active Directory forest to BPOS, synchronizing the GAL for users on both sides. User objects copied to the BPOS side are marked as disabled, so they can't be used to log on to BPOS, and they don't require licenses. You have to manually activate the accounts of users who you want to be homed on BPOS.

Microsoft's migration documentation calls for six steps in the coexistence setup process. Most of these steps have wizards to assist you through the process.

- Add your organization's domain to Microsoft Online Services. You'll have to add your domain to the Exchange Online domain list, then verify that you have control over the domain (usually by adding a CNAME record

with a unique ID that Microsoft assigns). Once you've done so, Exchange Online will be able to send mail from your domain by routing it to your servers. Note that this step may take longer than you expect because the DNS changes you make have to propagate.

- Enable Transport Layer Security (TLS) so that e-mail traffic between your servers and Exchange Online is encrypted. You'll need a certificate issued by a public certificate authority (CA). You can't use the self-signed certificates that Exchange automatically generates for its own internal use.
- Verify that email traffic is going where it should. The simplest way to do this is to send messages between a BPOS-hosted mailbox and one hosted on your local Exchange server.
- Turn on directory synchronization in the BPOS interface. You have to do this before installing the dirsync tool.
- Install and configure the dirsync tool. As part of the process, you'll need access to an account with Enterprise Admin rights; that account will be used to set up the MSOL_AD_Sync service account under which the dirsync tool actually runs.
- Wait three hours for the first dirsync pass to complete. By default, automatic dirsync from you to Exchange Online happens every three hours. Once you've determined that all the AD user and contact objects in your organization have been synchronized, you should make a change (perhaps adding a test user or contact), then force a manual synchronization to verify that it works as well.

At this point, you're ready to move mailboxes for those users whom you want in the cloud. Before you can do so, you must activate their accounts (acquiring licenses if needed) so that BPOS creates the needed Exchange store objects for the mailbox. Once the target accounts have been activated, you can use the BPOS tools to move their mailboxes. As soon as a mailbox is moved using the BPOS tool, mail for that user automatically begins to flow to the newly moved mailbox.

If you're migrating, you'll have a somewhat different to-do list depending on whether you're moving from an IMAP/POP environment or an Exchange organization. In the case of Exchange, most of the steps are the same as they are for coexistence, with the difference that eventually all of your mailboxes will be moved. IMAP/POP migration requires a fairly straightforward but tedious process of generating CSV files that tell the migration tools what mailboxes to migrate, what server they're on, and what credentials to use.

In both coexistence and migration scenarios, keep in mind that incoming mail will still be delivered to your on-premises Exchange organization. Exchange will reroute mail for BPOS mailboxes automatically. However, when you want all mail to flow to BPOS first (as you would during a complete migration), you'll have to manually repoint your DNS MX record to the BPOS servers, as well as enabling inbound messaging in the BPOS interface.

The future

Some of the coolest features enabled by hybrid scenarios aren't quite ready yet. That's because as of this writing, BPOS still uses Exchange 2007, and Live@EDU is using a pre-release version of Exchange 2010. However, based on my experience using Live@EDU's Outlook Live service, it's clear that Microsoft is committed to the hybrid model, and they're building a very strong base of experience and knowledge around running hybrid systems in production on millions of mailboxes. Exchange 2010 was expressly designed to be run either on premises or as a hosted service, so you should check out the hybrid model; you may find that it better fits your organization's requirements than what you have now.

Exchange 2010 Storage and Performance Improvements

by Paul Robichaux

One of the best features of Exchange 2007 was that it offered significantly better I/O performance than Exchange 2003. This was primarily due to three things:

- A change in the Extensible Storage Engine (ESE) page

size from 4Kb to 8Kb; for most messages, the larger page size offered a sizable reduction in the number of read or write operations required.

- The use of 64-bit versions of Windows, which allows ESE to use much larger amounts of RAM for caching. Because of the way ESE caches database pages, adding more RAM to the cache provides a dramatic boost in I/O performance. When you factor in the low cost of RAM compared to the cost of adding more disk spindles, the price/performance of RAM-based caching is even stronger.
- Internal changes to the format used for database pages and tables.

With these three changes, Exchange 2007 could perform up to 70 percent better under identical loads (meaning that the number of I/O operations per second, or IOPS, required for a given load was 70 percent lower) Exchange 2010 reduces the I/O workload by up to an additional 50 percent, meaning that for many sites, Exchange will effectively no longer be I/O bound. This raises some interesting possibilities for storage design.

The Role of Disks

Storage design is a complicated topic. Microsoft has built an Excel-based calculator that you can use to take a first cut at a storage design based on a given workload, and it will be updated for Exchange 2010. In the meantime, consider some of the changes in disk technology over the past few years:

- SATA-based drives are steadily increasing in capacity and throughput. As of this writing, 1GB server-class SATA drives are widely, and inexpensively, available and they offer throughputs of up to 1GB/second, equal to the best available Fibre Channel (FC) or serial-attached SCSI (SAS) for much less money.
- Sequential I/O throughput scales linearly based on the density of data recorded on disk. The denser the data, the more data can be read or written during sequential I/O operations. The introduction of perpendicular recording technology has allowed a massive increase in areal density, which is part of the reason large disks are so inexpensive.
- Random I/O performance is tied to how fast the disk heads can physically be moved from place to place. In turn, that rate is tied to the rotational speed of the disk and the mass of the heads. Rotational speeds are largely plateaued, and head masses are not likely to drop greatly barring a major technical breakthrough, so random I/O performance probably won't change much in the next three to five years.

Given these trends, Microsoft has chosen to optimize the Exchange 2010 database for a world where inexpensive SATA disks offer the best price/performance ratio.

Database Schema and Format Changes

There are a number of changes to the schema used for the Exchange databases (note that this schema is completely unrelated to the Active Directory schema, which is also heavily modified when you install Exchange 2010). The basic goal of the database changes was to stop doing lots of small disk reads and writes and instead do a smaller number of larger reads and writes. This takes advantage of the progress in disk I/O speeds over the past several years. The schema changes include

- keeping leaf pages that are related to one another physically contiguous on disk whenever possible
- storing all the database headers for a single mailbox in a single table instead of keeping separate tables for each folder in the mailbox. This allows consolidation of I/O for all folders in the mailbox.
- updating views and indices only when a user requests them. In Exchange 2007, the stored views and indices in a mailbox were updated every time a new message arrived. This change makes a major difference for users who receive lots of mail or who have lots of views.

There were also changes to the Extensible Storage Engine (ESE), the database engine that Exchange uses for mailbox and public folder databases. The changes here were focused on making database I/O requests be less random and more sequential to better take advantage of high read and write speeds on modern disks. To do this, ESE was modified to automatically reorder pages to make them sequential, and some database pages (those containing long value streams, or LVs) are now compressed. The database page size itself was also increased. Exchange 2003 and earlier used a 4Kb

page size, and Exchange 2007 used an 8Kb page. Exchange 2010 now uses 32Kb pages.

Another change is that the online defragmentation process familiar in Exchange 2003 and Exchange 2007 is now gone, and several operations normally performed during the nightly maintenance window are now performed in the background when necessary. Eliminating the maintenance window was necessary to provide better performance during failovers and to reduce the amount of time when many pages in the database are undergoing near-simultaneous changes—that causes problems for database replication.

Overall, these changes can provide up to a 50 percent reduction in the number of I/O operations required for a given workload!

Introducing Database Availability Groups

Another huge change in Exchange 2010 is the introduction of a new high availability mechanism: database availability groups (DAGs). The concept behind the DAG is pretty simple: you can now keep replicas of any mailbox database on any Exchange server in your organization. A given database can have up to 16 replicas, and the replicas can be hosted across AD site boundaries. While this sounds pretty revolutionary, it's actually a logical extension of the combination of two Exchange 2007 features: clustered continuous replication (CCR), which provided data replication between cluster nodes, and standby continuous replication (SCR), used for cross-site replication. CCR and SCR are no longer available (and neither is local continuous replication). The traditional clustering mechanism (which Exchange 2007 called single-copy clusters) is also gone. Perhaps the most surprising change related to the DAG is that there are no longer storage groups—every database has its own associated set of transaction logs.

In practice, this means that much of the pain of building high-availability Exchange environments vanishes. To enable a DAG, you create a DAG and then add database replicas to it. You don't have to manually create any of the failover mechanisms, install any Windows prerequisites, or any of the other things you'd have to do with single-copy clusters. A new Exchange component called the Active Manager tracks which database copy is mounted at any given time, mounts databases when necessary, and keeps track of which servers have mounted which databases when. The Exchange 2010 client access server (CAS) queries Active Manager to find the current active copy of a database so that it can point clients to it.

The Active Manager allows you to change DAG membership and contents at any time, and it eliminates the need to ever use the Windows clustering management tools. You can manually make a given copy of the database active (Microsoft calls this a switchover), or Active Manager can make a copy active when it detects a failure related to the currently active copy (this automatic operation is called a failover).

When you create a DAG, you're creating a new AD container that represents the DAG as a collection of mailbox servers. You then add servers to the DAG. When you add the first server, Exchange silently sets up a Windows failover cluster (which is why using DAGs requires the Enterprise Editions of both Windows and Exchange). Once you have added all the servers you want as DAG members, you can start specifying which servers should have replicas of which databases.

As you add additional copies of the database to other servers, Exchange automatically seeds the new copies using the ESE streaming APIs (which is considerably more efficient than the TCP-based mechanism used in Exchange 2007), then replicates changes using one socket per database. DAG replication traffic uses Kerberos authentication and encryption, and replication traffic can be compressed. DAG design calls for two networks to be available to each mailbox server: one for replication traffic and one for MAPI communication with other mailbox servers. The Active Manager is smart enough to automatically move replication traffic to the MAPI network if the replication network fails. If the MAPI network fails, a healthy copy of the database will be activated on another node.

Apart from being technically sweet, the DAG architecture offers some very impressive advantages. First, it is much simpler to deploy and maintain than traditional clusters. That's an important benefit, especially for companies that want better availability than individual servers can provide but that lack in-house skills to deploy shared-storage clusters.

Second, because a DAG-hosted mailbox database is fully replicated to every node, you can back it up from any node, not just the active copy. Third, DAGs can be set to lag replication by a certain amount of time (just like CCR/SCR in Exchange 2007), so that you can build topologies that replicate data only after you know it's good. Fourth, the user experience during a failover or switchover is greatly improved because the amount of time required to switch active copies is reduced—it takes about 30 seconds to make the switch, and the amount of time required isn't dependent on the volume of logs that have to be played back.

Storage Design in Exchange 2010

Given the changes in disk technology, and the new features in Exchange 2010, you might think that there are some changes in how you design storage systems to support Exchange 2010. Exchange 2010 is largely optimized for designs that use JBOD technology: Just a Bunch Of Disks. Instead of taking multiple disks and building a RAID array, you take the same number of disks and use them as independent volumes. If a disk fails, there's no protection for it.

Sounds crazy, doesn't it? It's not! DAGs offer the ability to maintain multiple copies of mailbox databases distributed across an organization in whatever manner you like. Rather than building a RAID array on one server, take the same number of disks and spread them across two servers—that gives you not only storage protection (since a single disk failure will cause a DAG failover) but the benefits formerly reserved for clustering. For example, you can cause a DAG switchover to do maintenance on one server, then switch back and you're protected against server failures by the automatic DAG failover mechanism. In order to make this a possibility, Microsoft had to make a number of changes to reduce the impact of a failover. This effort was largely concentrated on reducing the impact of re-seeding a replicated database after a failover. These improvements pay off, of course, in many other circumstances.

This is not to negate the role of a properly provisioned and maintained SAN. A good SAN offers a number of benefits, including flexible storage reallocation, hardware-level replication, and hardware-based point-in-time copies. As well, SANs give you a flexible storage architecture that can support multiple applications on a single storage pool. However, Exchange 2010 offers the realistic option of hosting highly available, large-scale Exchange deployments without requiring SANs either for I/O performance or data protection—a welcome option.

The bottom line is that it's too early to authoritatively state a best practice for storage designs with Exchange 2010. Microsoft has a wealth of data gathered from the nearly 4 million users hosted on Outlook Live, Live @ EDU, and early-adopter customers, but those data are skewed toward large-scale hosted environments. It will take some time for the best practices for smaller deployments to be proven in the real world.

DAG Likely to be Widely Adopted

Microsoft has made some major changes to the database subsystem in Exchange. Compared to Exchange 2007, these changes give significantly better I/O performance for the same workload. At the same time, the changes support a radically new high availability model that reduces the cost and pain of designing HA Exchange systems. The DAG system is likely to be widely adopted because of its benefits, and it's worth considering an upgrade to Exchange 2010 for that feature alone.

the bigger OEMs have some feature they've invested in and want it to be exploited or made available through the release. I think we have 1,200 Windows Hardware Quality Lab certified servers for 2008 R2 already, which is much more than we've had before.

I'm very pleasantly surprised with how smooth the move to 64 bits has been. We made that decision about four years ago—I think we announced it at TechEd 2005—and said 2008 would be the last 32-bit, and we'd try to move people. As far as I can tell, it has gone very smoothly—we're not seeing any hiccups, the drivers are all available. You might hear otherwise from your readers, but again our telemetry was telling us what we could see was happening with 2008.

Michele Crockett: What does Server 2008 R2 offer for people who are leaning more toward Linux, either users already on Linux or that have been a bit fickle?

Bill Laing: There's a couple of things. I always say to people: focus on delivering value. When you look at the total cost that people spend on IT, the actual procurement cost of the hardware and software is a pretty small percentage. I've seen numbers between 10 percent and 18 percent. So if you focus on price, that's interesting; but if you can help people with the other 85 percent to 90 percent, reduce their costs, and make their lives easier, that's better. I'll often say, "Let's figure out features that give IT pros back an hour of their day." That's actually worth more to them than the original cost.

And also, there's the fact that we have an integrated system—you can put a number of roles together. I think we still have a very strong directory, which is a big part of the infrastructure. We play well with the clients. So I believe that, ultimately, people make rational economic decisions over the long term. But it's like saying the stock market is rational over the long term.

Michael Otey: What are the most popular roles being deployed? What percentage of Windows systems are running multiple roles such as file server or active domain controllers?

Bill Laing: It varies depending on the size of the business. Enterprises tend to be more dedicated per role. Branch offices are a funny case because they behave like small businesses, but they are an enterprise deployment and they tend to put multiple roles together. So we've seen the Read Only Domain Controller plus File and Print Server, and maybe running an application locally in a branch or small office.

Similarly, they might have a web server because they have SharePoint. And at the high end, enterprises are more likely to say, "This is my web server, this is my directory server," and that's why we came up with the term *role*. When we would interview people, they'd say, "This is my . . ." And they'd point to the machine.

So we have a reasonable spread—it's the ones you might think of, such as file and print, web, that are all fairly created shares. Terminal Services is a popular deployment role as well. Virtualization is something else we're seeing that's changing the dynamic there a little bit: people are saying, "It's nice to keep things separate but still consolidate them on one machine." Because there's always, "If I change this for this role, are there any side effects to other roles?" You can put them in a separate VM and still get that benefit.

Michael Otey: In some ways, virtualization could let you more easily have one server per role because then you have a virtual machine that's your web server, another one that's your Active Directory, and so on.

Bill Laing: Yes, and it's easier to do your upgrade or make some configurations if they're really only for a web server and not your domain controllers, for instance. It's interesting that with R2 the domain controller is very compatible, so we tested with earlier versions of Exchange, the latest version of Exchange, earlier versions of Active Directory, and we've learned that trying to change the infrastructure really slows down deployments. And you can say that you can really happily go from NT 4.0 to Windows 2000, but by the way you have to roll out this new domain structure. It's really hard to get the deployments then. And you can just do the features you want for Direct Access, and you can just put that part to support your Windows 7 clients, or put in a Branch Cache for a Windows 7 client.

I think the momentum around Windows 7 has helped. It's undoubtedly a very positive response from people. It really is a very exciting system whether you're an IT person or an end user—we're seeing a lot of excitement from them.

Michael Otey: Server 2008 R2 has an incredible number of features. If you were to pick, what would you say are the top three value-adds for your customers?

Bill Laing: In priority, it would be virtualization and Live Migration. I think the power management work we've done is a slow burner people will appreciate over time. And I like the more extensive PowerShell coverage.

Michele Crockett: What customer scenarios did not make it into this release that really broke your heart or that you're looking forward to including in the next release?

Bill Laing: I don't think anything broke my heart—we're just starting to retrench and get feedback from people on what they want. I think we learned a lot about the process—we've improved our maturity and planning process. Really being connected to customers and partners is key—if you're not building something they want, maybe you're not going to be the king of the market. I think we feel very attuned to that. We have a pretty well-developed process for collating our feedback, as well as telemetry, and the competition is Linux and VMware. It's somewhat simpler than it used to be in some sense.

InstantDoc ID 103404

Michele Crockett
(michele.crockett@penton.com) helped launch *SQL Server Magazine* in 1999, has held various business and editorial roles within Penton Media, and is currently editorial and custom strategy director of *Windows IT Pro*, *SQL Server Magazine*, and *System iNEWS*.

Michael Otey
(motey@windowsitpro.com) is technical director for *Windows IT Pro* and *SQL Server Magazine* and coauthor of *Microsoft SQL Server 2008 New Features* (Osborne/McGraw-Hill).

Using Active Directory Administrative Center in Windows Server 2008 R2

by Jan De Clercq

ADAC offers time-saving features for admins

Windows Server 2008 R2 includes new features that can simplify the way you administer and maintain Active Directory (AD). Besides the AD Recycle Bin—a great feature for AD object recovery—and the AD Best Practices Analyzer—a very valuable tool for AD health checking—one of the most eye-catching new management-related features is certainly Active Directory Administrative Center (ADAC). Let's look at this new tool and see how ADAC can help simplify your day-to-day AD administration work.

ADAC can be installed only on computers running Server 2008 R2 and is available with Windows Server 2008 R2 Standard, Enterprise, and Datacenter Editions, but not the Itanium and Web Server Editions. ADAC is installed by default when you install the Active Directory Domain Services (AD DS) server role. ADAC is also included in the Remote Server Administration Tools (RSAT) feature.

How ADAC Differs From ADUC

ADAC offers administrators a good alternative to the Active Directory Users and Computers (ADUC) Microsoft Management Console (MMC) snap-in for managing AD objects. As with ADUC, administrators can use ADAC to perform common AD user, computer, group, and organizational unit (OU) object management tasks. Like ADUC, the current version of ADAC is used only for managing AD DS instances and not for managing Active Directory Lightweight Directory Services (AD LDS, formerly Active Directory Application Mode—ADAM) instances.

The key difference is that ADAC is a very task-oriented administration tool that can help you manage AD in fewer steps. The ADAC interface focuses on key AD administration tasks. For example, two very frequently performed tasks, resetting a password and searching AD for an object, are immediately available when you open ADAC, as Figure 1 shows.

With ADUC, to reset a password you first had to locate the object, then right-click it and select Reset Password, and only then could you enter the new password data. In ADAC you can perform all these tasks in a single action from the ADAC opening screen.

ADUC is, foremost, a data-oriented tool: It shows you how the data in AD is organized. ADAC supports this data-oriented view of AD objects as well. The classic hierarchical view of AD content is available from ADAC's treeview, which I discuss in more detail later in the article.

Besides the ADAC interface's focus on key administration tasks, two other important differences you will notice in the interface are that ADAC is much more customizable, and it lets you simultaneously connect to other domains. ADUC supported taskpads but these were never a big success, and it required different instances to be able to manage objects across multiple domains. ADAC lets you simultaneously connect to different domain

controllers (DCs) in different domains to manage objects across multiple domains within the same ADAC instance.

The other big difference between ADUC and ADAC lies in ADAC's underlying architecture. ADAC is not MMC-based but uses an Explorer-like interface instead. Under the hood, ADAC leverages Windows PowerShell and the new Active Directory Web Services. ADWS is a new Windows service that provides a web service interface to AD.

To use ADAC, you need at least one Windows DC in your domain that has an operational ADWS service. ADWS is included in Server 2008 R2, and Microsoft also provides an ADWS add-on package for Windows Server 2003 SP2, Windows 2003 R2 SP2, Server 2008, and Server 2008 SP2. This package is called the Active Directory Management Gateway Service. You can get it from www.microsoft.com/downloads/details.aspx?FamilyID=008940c6-0296-4597-be3e-1d24c1cf0dda. This means that you can also use ADAC to manage AD instances that are running on other Windows server platforms other than Server 2008 R2.

Server 2008 R2 includes a new set of powerful PowerShell cmdlets for AD administration that are bundled in the Active Directory Module for Windows PowerShell. This module calls on the Microsoft .NET Framework 3.5.1 and ADWS for accessing the AD core engine.

Server 2008 R2 automatically installs the PowerShell engine, the Active Directory Module for PowerShell, the .NET Framework 3.5.1, and ADWS when you install AD DS. You also get access to these services when you add the RSAT feature to a Server 2008 R2 or Windows 7 machine. RSAT is bundled with Server 2008 R2. For more information about RSAT for Windows 7, go to support.microsoft.com/default.aspx/kb/958830. You can download RSAT for Windows 7 at www.microsoft.com/downloads/details.aspx?FamilyID=7D2F6AD7-656B-4313-A005-4E344E43997D.

Exploring ADAC

You can find ADAC in the Administrative Tools folder of your Server 2008 R2 server Start menu or you can start it from the command line using dsac.exe. When ADAC opens, it shows the Administrative Center Overview page that's illustrated in Figure 1. There, you can find three sections: Reset Password, Global Search, and Getting Started. Often these are the three tasks an AD administrator performs most. You can customize the Overview page by adding or removing certain of these sections. To do so, use the Add Content drop-down button in the top right corner of the Administrative Center Overview page.

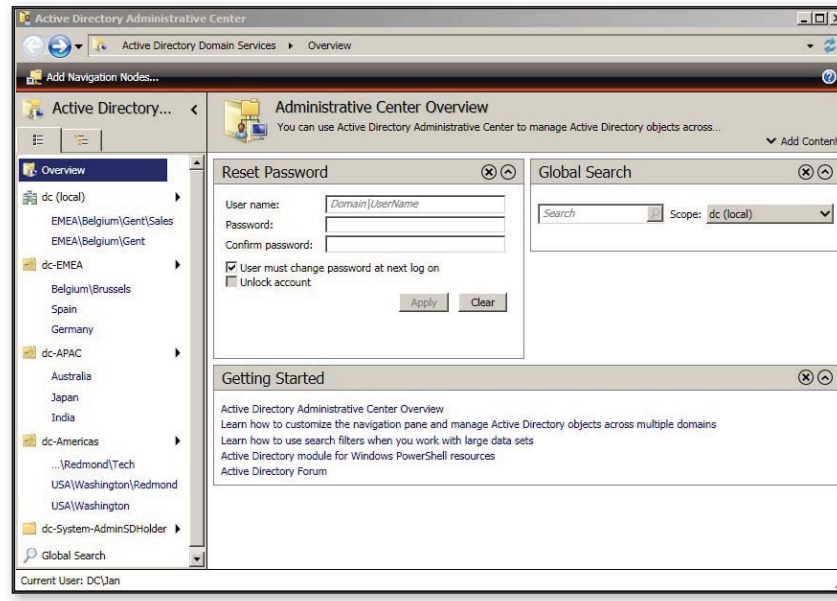


Figure 1: Administrative Center Overview page

On the left side of the Administrative Center Overview page are the ADAC navigation pane and your personal navigation nodes. Navigation nodes are shortcuts to containers in the local AD domain or its trusted AD domains. When you click a navigation node, ADAC takes you right to the corresponding AD container and displays its content in the right pane, which Figure 2 shows. To create your personal navigation nodes, click Add Navigation Nodes at the top of the navigation pane. Again, you

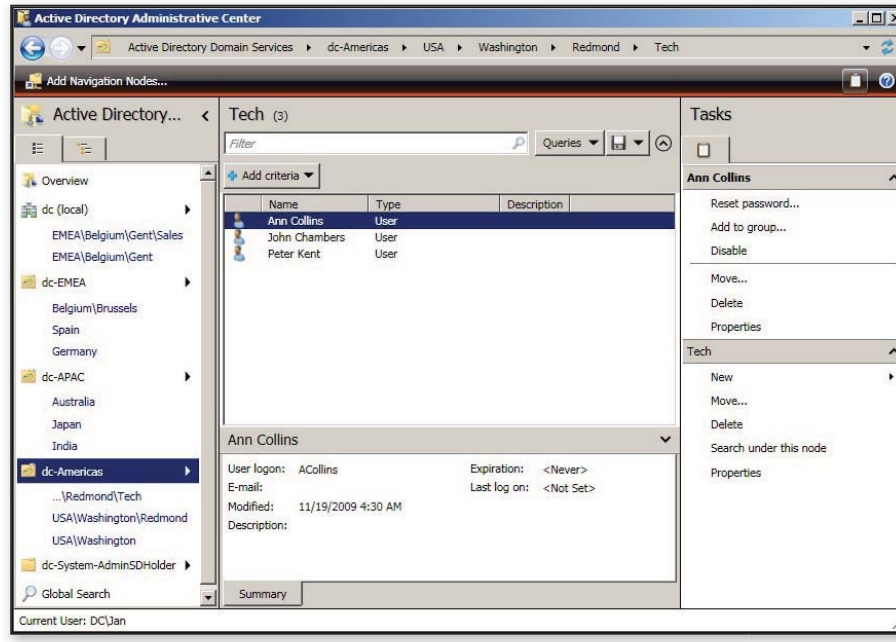


Figure 2: List view with personal navigation nodes

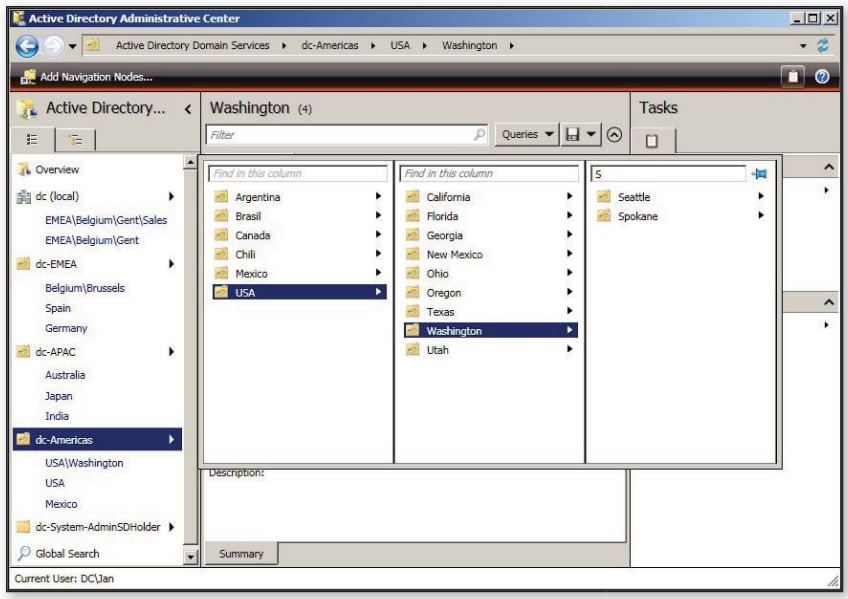


Figure 3: List view with Column Explorer

can customize the navigation pane: When you right-click a navigation node you can rename or remove the node, create a duplicate node, or move the node up or down in the navigation pane list.

You can browse the navigation pane and its nodes using a treeview, which is similar to the ADUC console tree or by using the new list view. If you're used to the ADUC console tree, it's a bit confusing that the ADAC treeview also shows all your navigation nodes. This means a given AD container can show up multiple times in the ADAC treeview. You can switch between the ADAC list and treeview by using the two tabs at the top of the navigation pane: List view is the left tab; treeview is the right tab.

In the ADAC list view you can use the Column Explorer feature that provides a Start menu–like view on the AD container hierarchy, which Figure 3 shows. Column Explorer simplifies browsing through the AD hierarchy because it displays all child containers of a given parent container in a single column and adds new columns as you dig deeper in the AD hierarchy. Column Explorer also provides a *Find in this column* box where you can type the name of the container object you're looking for. ADAC automatically filters the current view while you type.

As you can see in Figure 3, I searched for the Seattle OU, and ADAC automatically filtered the content of the Washington OU to the Seattle and Spokane OUs while I typed the letter S in the *Find in this column* box. This can be a very useful feature when dealing with large data sets: You no longer need to scroll through the entire list of OUs to locate a particular OU. Another hidden ADAC change that's important for dealing with large AD data sets is that ADAC gets rid of the OU display limit of 2,000 objects per OU that ADUC set.

The list view also has a Most Recently Used (MRU) feature that shows the last three containers you accessed in a particular navigation node. In the example in Figure 2, my MRU containers for my EMEA navigation node were Belgium\Brussels, Spain, and Germany.

Server 2008 R2 includes a new set of PowerShell cmdlets for AD administration that are bundled in the Active Directory Module for Windows PowerShell.

At the top of the ADAC window is the breadcrumb bar. It lets you navigate directly to a specific container in your local domain or in a trusted AD domain by specifying an LDAP path, a distinguished name (DN), or a hierarchical path to an AD container. Figure 2 shows a hierarchical path to the \Active Directory Domain Services\dc-Americas\USA\Washington\Redmond\Tech container in the breadcrumb bar. You can use this bar to navigate only to containers that are part of the domain AD naming context of your local domain or a trusted domain. You can't use it to navigate to containers of the configuration, schema, or application AD naming contexts. The breadcrumb bar is a feature that can be very handy when you must administer large AD data sets.

More Customization

When you open the properties of an AD object in ADAC (which you can do by double-clicking the object or by clicking the Properties link in the Tasks pane), you will notice that the property page is very different from what it was in ADUC. This is illustrated in Figure 4 for the Peter Kent user object. ADAC shows only the most important object properties and groups the properties in sections.

To perform common administrative tasks such as an object rename or move, or a password reset, you can use the Tasks drop-down menu on the top right of the property page. In case you can't get used to the new property page, the classic tabbed ADUC view of an AD object's properties can be found in the last section of the ADAC property page called Extensions. However, you can only use this tabbed view to administer the object properties that aren't already contained in the other sections.

Again, ADAC lets you easily customize an object's property page. You can display or hide property page sections by using the buttons on the top right of each section or by using the Add Sections drop-down menu at the top right of the property page.

For AD administrators, it's paramount to have a powerful AD search engine. The ADAC search engine is called Global Search and is both flexible and powerful. You can access it from the Administrative Center Overview page or by using the Global Search link on the navigation pane.

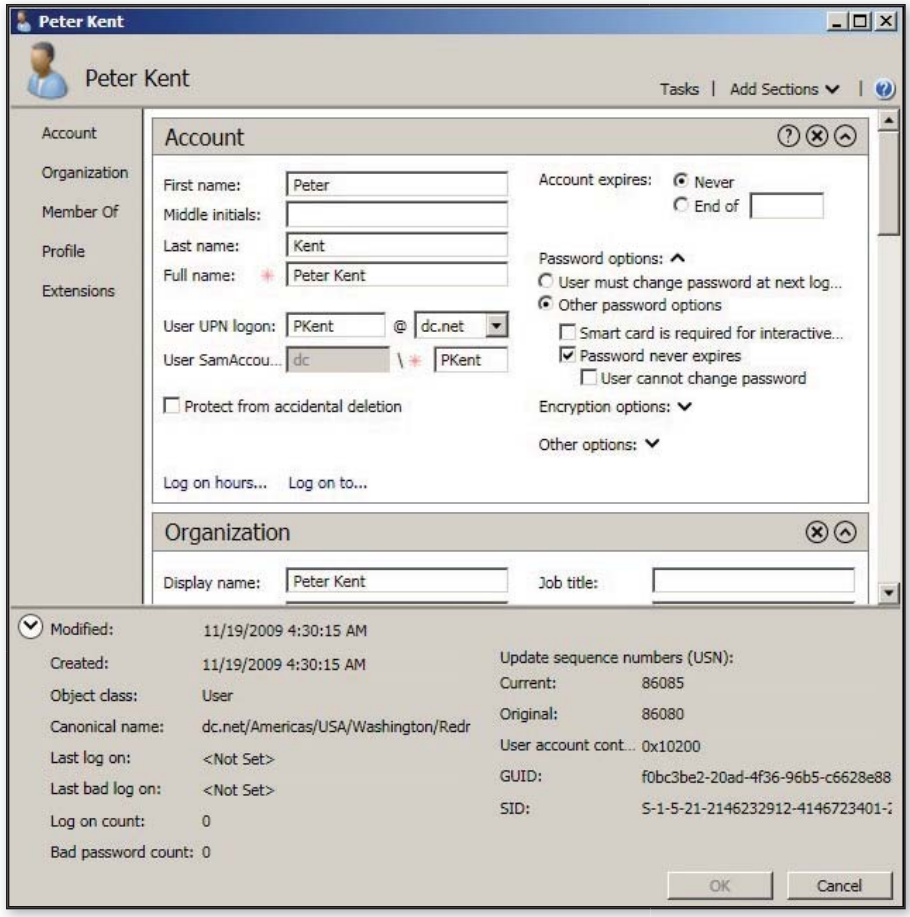


Figure 4: User object properties screen

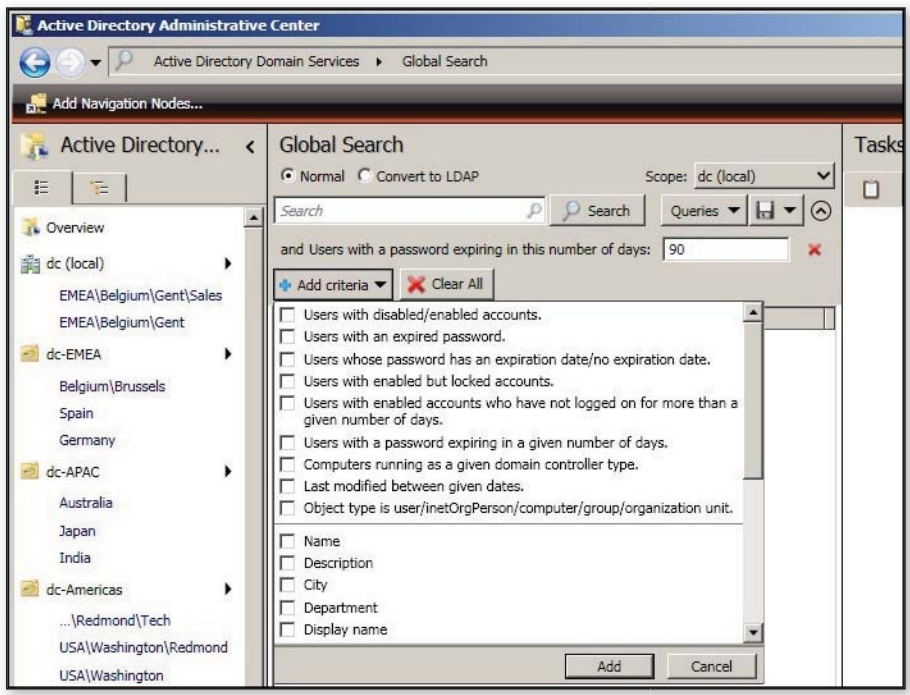


Figure 5: Using Global Search

From the Global Search page, which Figure 5 shows, you can build AD queries using specific keywords and search criteria. You can use predefined criteria such as *Users with a password expiring in this number of days* or *Users with enabled but locked accounts*. When you select the *Convert to LDAP* option, Global Search converts the search criteria you selected to an LDAP query string that you can then fine-tune in the *Enter LDAP query* window.

Global Search also lets you save your queries and reuse them. To save your query, use the Save button at the top right of the Global Search page. To retrieve a query that you previously saved, use the Queries button.

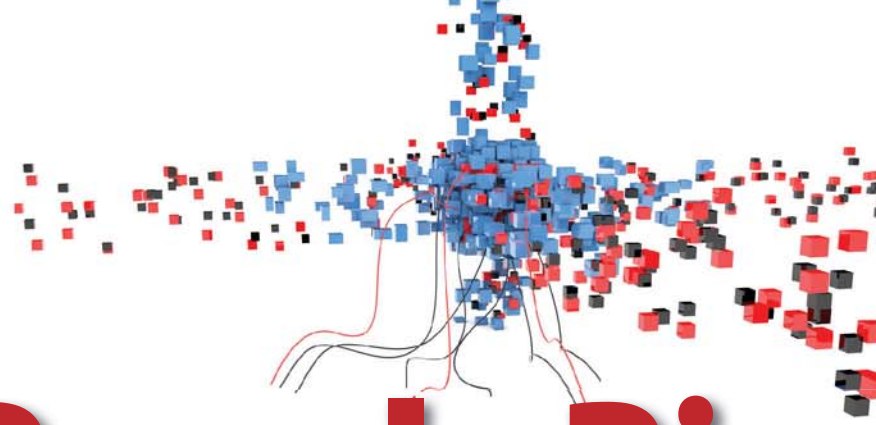
Impressive First-Version Product

ADAC offers a single administration interface for connecting to different domains and provides efficient tools for searching and locating AD objects in a large AD database. However, the ADAC interface is very different from ADUC, and it will definitely take some time to get used to it.

One small thing I found missing from the ADAC interface is a refresh option—this can be handy when you're using ADUC and ADAC simultaneously and you add or modify objects in ADUC. Also, for the automation of certain AD administrative tasks, it would have been nice to have access to the PowerShell code that's underlying ADAC. ADAC is an impressive first-version product and a welcome addition for AD administrators who must deal with large AD databases and many AD domains.

InstantDoc ID 103244

Jan De Clercq
(jan.declercq@hp.com) is a member of HP's International Expertise Team and focuses on architecture for Microsoft-based IT infrastructures, identity management, and security. He's co-author of *Microsoft Windows Security Fundamentals* (Digital Press).



AD Recycle Bin FAQs

by John Savill

Quick answers to your questions about the Active Directory Recycle Bin

Q. What is the Active Directory (AD) Recycle Bin in Windows Server 2008 R2?

A. Server 2008 R2 introduces a number of new AD features, and the AD Recycle Bin is one of the features getting the most attention.

Normally, when an AD object is deleted, it's tombstoned—the object is marked as deleted, this tombstone status replicates to all domain controllers (DCs), and after the tombstone lifetime passes, the object is actually deleted by the garbage collection process. As soon as you delete an object, most of its attributes are removed and all linked value attributes, including group memberships, are deleted. If you want to recover a deleted object, you can boot a DC into Directory Services Restore Mode, restore a backup, and then mark an object (or objects) as authoritative, which will bring the object back. An alternative approach is to reanimate a tombstoned object, which removes the tombstone status and makes the object available again. However, the reanimated object will have lost all group memberships and most attributes (but will keep the same SID).

In Server 2008 R2, you can enable the AD Recycle Bin to change this lifecycle, which Figure 1 illustrates. When an object is deleted with the AD Recycle Bin enabled, none of its attributes or linked value attributes are deleted. Its name is mangled slightly, the isDeleted attribute is set to TRUE, and the object is moved to the Deleted Objects container. While the object is in the Deleted state, it can be undeleted with no loss of attributes or group memberships using a PowerShell cmdlet or the Ldp tool.

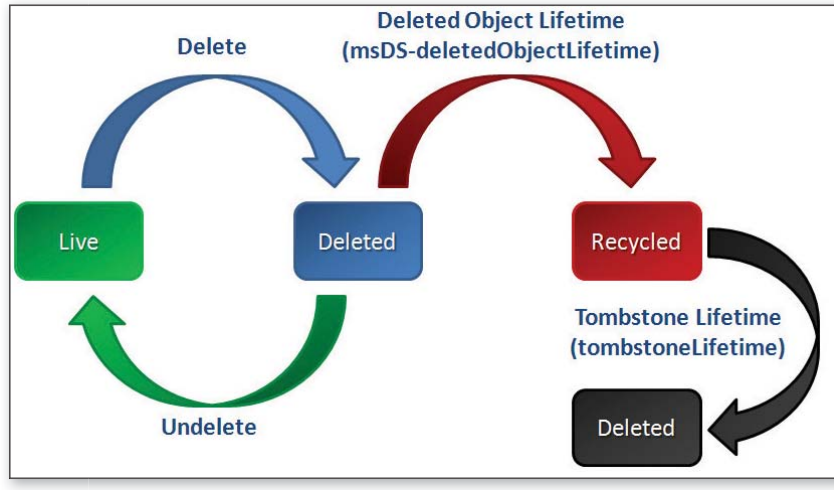


Figure 1: The AD Recycle Bin lifecycle

The object stays in this state for the duration set in msDS-deletedObjectLifetime, which by default is the same as the duration of tombstoneLifetime, 180 days. When the deleted object's lifetime has passed, it moves into a recycled state. In this state, its isRecycled attribute is set to TRUE, linked value attributes (such as groups) are removed, and most of its normal attributes are removed, the same as in systems without Recycle Bin. The object can't be restored through any means after it enters this state, and it's physically deleted by garbage collection when the tomestoneLifetime passes.

Note that the AD Recycle Bin requires the forest mode to be Server 2008 R2, so every DC in the forest must be running Server 2008 R2. Also, after you enable the Recycle Bin, you can't disable it.

InstantDoc ID 102221

Q. How do I enable the Active Directory (AD) Recycle Bin?

A. Once you've raised your forest's level to Windows Server 2008 R2, you need to use the Enable-ADOptionalFeature cmdlet to enable the Recycle Bin for the forest. Remember, when you enable this feature, you can't disable it, so be sure you really want this functionality.

The format of the command is shown here:

```
Enable-ADOptionalFeature -Identity
  'CN=Recycle Bin Feature,CN=Optional
  Features,CN=Directory Service,CN=
  Windows NT,CN=Services,CN=
  Configuration, DC=<your domain>,
  DC=<net or com>' -Scope
  ForestOrConfigurationSet -Target
  '<DNS name of forest>'
```

You can see if the Recycle Bin is enabled by viewing the AD optional features:

```
Get-ADOptionalFeature
  -filter {name -like "*"}
```

You'll see in the output from this command that there are no enabled scopes for the Recycle Bin, so the Recycle Bin isn't enabled. I now enable the feature:

```
Enable-ADOptionalFeature -Identity
  'CN=Recycle Bin Feature,CN=Optional
  Features,CN=Directory
  Service,CN=Windows NT,CN=
  Services,CN=Configuration,DC=
  savilltech,DC=net' -Scope
  ForestOrConfigurationSet -Target
  'savilltech.net'
```

When you enter this command, you'll receive the following message:

```
WARNING: Enabling 'Recycle Bin
  Feature' on 'CN=Partitions,CN=
  Configuration,DC=savilltech,DC=net'
  is an irreversible action!
```

You'll be asked to confirm your action; select Y from the list of options to proceed, and the recycle bin is now enabled. You can verify this in the AD optional features—you'll see that the Recycle Bin now has enabled scopes.

InstantDoc ID 102222

Q. If I create a new Windows Server 2008 R2 forest and select Server 2008 R2 functional mode, is the Active Directory (AD) Recycle Bin enabled automatically?

A. No. Optional features are never enabled automatically. You need to enable the AD Recycle Bin manually, using the Enable-ADOptionalFeature cmdlet or Ldp.

InstantDoc ID 102738

Q. How can I view Active Directory (AD) objects in the Deleted state after the AD Recycle Bin is enabled?

A. The Get-ADObject PowerShell cmdlet can be used to view deleted objects if you pass the switch -IncludeDeletedObjects. Alternatively, for more general browsing, you can use the Ldp tool. To view deleted objects, you have to enable the *Return deleted objects* control, which is available in the Controls menu under Options.

When this setting is enabled, you can browse the tree by connecting, binding, and then viewing the tree with the base distinguished name of the domain. Deleted objects in your domain will have isDeleted set to TRUE. You can actually take this a step further and enable the return of recycled objects in the Ldp controls. In this case, you'll see an isRecycled attribute, set to TRUE, and fewer attributes overall.

InstantDoc ID 102223

Q. How do I undelete an object from the Active Directory (AD) Recycle Bin?

A. If you've enabled the recycle bin, you can undelete objects that were both deleted after the recycle bin was enabled and that are still within the deleted object lifetime. To restore an object in the deleted state (isDeleted TRUE), simply pass the deleted object to the Restore-ADObject cmdlet. The easiest way to pass the object is to use the Get-ADObject cmdlet and pass the -IncludeDeletedObjects switch.

For example, if I know the displayName of an object is Dick Grayson, I would use the command

```
Get-ADObject -Filter
  {displayName -eq "Dick Grayson"}
  -IncludeDeletedObjects |
  Restore-ADObject
```

If you stick with first-party solutions, you can only undelete from the AD Recycle Bin using the Restore-ADObject PowerShell cmdlet, not from the GUI.

InstantDoc ID 102224

Q. Is there a graphical utility to access the Windows Server 2008 R2 Active Directory (AD) Recycle Bin?

A. Overall Solutions provides a free GUI for the AD Recycle Bin at overall.ca/adrecyclebin. The utility is a single executable. Click the Load Deleted Objects button and the utility looks for deleted objects and displays what it finds. You can then select the objects you want to undelete and click the Restore Checked Objects button. The utility seems to work great.

InstantDoc ID 102418

John Savill

(john@savilltech.com) is an advisory architect for EMC's Microsoft consulting practice. He's an MCITP: Enterprise Administrator for Windows Server 2008 and a 10-time MVP. His latest book is *The Complete Guide to Windows Server 2008* (Addison-Wesley).

PowerShell and Active Directory

by Darren Mar-Elia

A Powerful Combination in Windows 7 and Windows Server 2008 R2

Since its release, Windows PowerShell has become the automation platform of choice for Windows. Its power and flexibility have been proven in many environments and against many Windows technologies. Unfortunately, when it came to Active Directory (AD) support, PowerShell 1.0 didn't offer much functionality out of the box. Basically, Microsoft provided the ADSI "type-accelerator" and that was about it. If you needed to perform more advanced tasks, you had to access the native .NET classes that provided AD support—which required more advanced skills than most administrators were interested in learning. Many shops turned to third parties such as Quest Software and its AD PowerShell snap-in to fill the bill.

But with the release of Windows 7 and Windows Server 2008 R2, the wait for full-fledged PowerShell AD support is over. Microsoft has shipped an AD module and PowerShell drive provider in these new releases to make managing AD from PowerShell a snap.

How Do I Get It?

If you install a Server 2008 R2 domain controller (DC) by adding the Active Directory Domain Services role within Server Manager, the AD PowerShell module will be installed by default. However, if you want to install the module (a module is a just a collection of PowerShell cmdlets, providers, scripts, and so on) on your Windows 7 workstation, you'll need to install Remote Server Administration Tools (RSAT), which you can download from the Microsoft Remote Server Administration Tools for Windows 7 page (www.microsoft.com/downloads/details.aspx?FamilyID=7D2F6AD7-656B-4313-A005-4E344E43997D).

Once you've installed RSAT, go to the Control Panel Programs and Features applet, choose *Turn Windows features on or off,* and scroll down until you see the RSAT node. Expand the node until you see the Active Directory Module for Windows PowerShell node, as shown in Figure 1. Select the check box, then click OK to add the module.

Once the module is installed, you can select either the Active Directory Module for Windows PowerShell item from the Start menu, Program, Administrative Tools program group, or you can easily add it to your existing PowerShell session by typing:

```
Import-module ActiveDirectory
```

After a brief flash, the prompt will return and you'll be able to access all the power that PowerShell and AD have to offer. However, before we start using the AD PowerShell module, let me add one important piece of information. Unlike any prior implementations that allowed PowerShell-based AD automation, this new module requires that you have at least one DC in your

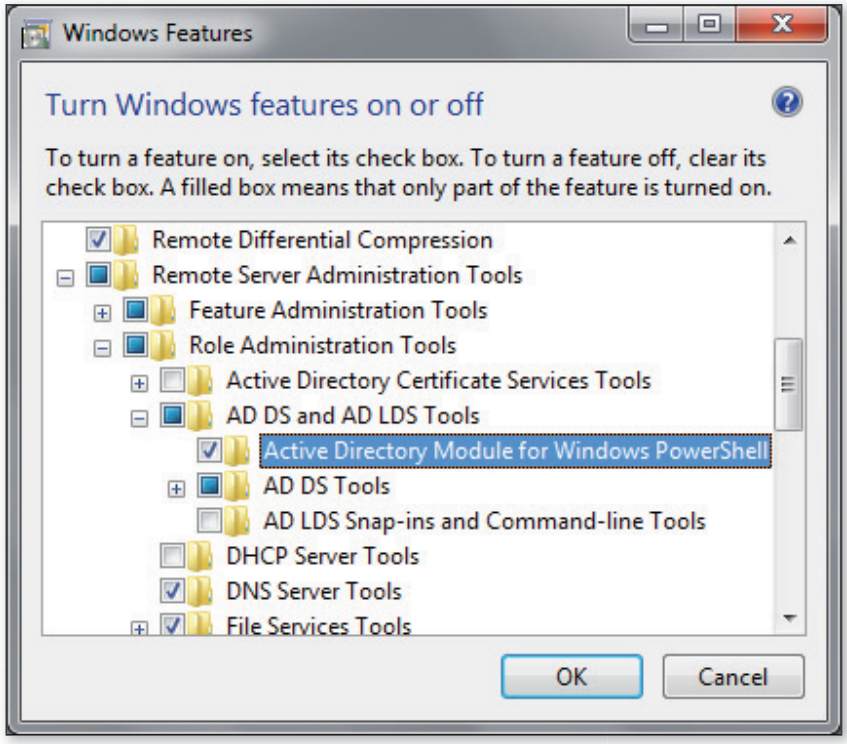


Figure 1: Adding the AD PowerShell module to Windows 7

domain running the new Active Directory Web Services. ADWS is installed by default on a Server 2008 R2 DC, but you'll need a special add-on to your Windows Server 2003 or Server 2008 DCs in order to use the module. You can download that module at www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=008940c6-0296-4597-be3e-1d24c1cf0dda.

If you don't have an ADWS server in your domain, you'll get an error when you try to import the AD module into PowerShell. The interesting thing to note about ADWS, and these PowerShell cmdlets in general, is that they don't use LDAP to talk to AD. Specifically, they use XML Web Services–based protocols to interact with AD. This is a significant departure from all previous AD toolsets and it will be interesting to see if Microsoft continues this trend in future AD management tools. Note that once you install ADWS on your non-Server 2008 R2 DC, you'll still be able to manage these servers using normal LDAP-based tools such as Active Directory Users and Computers.

Using the Cmdlets

Once you've installed the cmdlets and have a DC with ADWS running, you're ready to explore the power of PowerShell for AD. Microsoft provides two main tools for automating AD management using PowerShell. The first is a set of cmdlets that let you do everything from searching for AD objects to creating computer accounts to modify user accounts. The second tool is a PowerShell drive provider for AD that lets you navigate AD like a file system. This tool can be powerful for interactive use; I'll show you some nifty things you can do with it against AD.

> A powerful feature of PowerShell and the AD cmdlets is the ability to pipe output from one cmdlet to another.

Let's start by looking at some of the AD cmdlets. If you want a list of all the AD-related cmdlets exposed by the AD PowerShell module, open PowerShell and type the following:

```
get-command -module ActiveDirectory
```

This will return a list of 76 cmdlet names that are part of the AD module. As you'll see from the list, there are obvious cmdlets such as Get-ADGroupMember to retrieve members from groups and New-ADComputer to add computer accounts to the domain. Let's take a look at how you can use a few of these cmdlets. Let's say you want to quickly retrieve a list of members from the Marketing Users group in your domain. You can do that easily by using the following cmdlet:

```
get-ADGroupMember -identity "Marketing
  Users"
```

The identity parameter is common throughout the AD cmdlet as a way of referencing a particular AD object. The identity parameter can take the form of a distinguished name (e.g., DC=cpandl,DC=com), an object GUID, SID, or samAccountName.

Another powerful feature of PowerShell, and of these AD cmdlets, is the ability to pipe the output from one cmdlet to another. For example, let's say you want to find a user object in AD, and then disable that user object. You know the user's samAccountName is kmyer, so you can use the following two cmdlets to accomplish the task:

```
get-ADUser -identity kmyer |
  Set-ADUser -enabled $false
```

In this example, we're using the get-ADUser cmdlet to search for the user account with a samAccountName of kmyer. Once we find that user, we pipe it to the Set-ADUser cmdlet and pass it the parameter—enabled with the PowerShell $false flag to indicate that we want the account to be disabled.

This is a simple example that illustrates the power and simplicity of PowerShell and the AD cmdlets. Because this module contains 76 cmdlets, you can do a lot more with this feature. Let's look at one more feature within this module that's worth exploring: the Active Directory PowerShell drive provider.

The Active Directory PowerShell Drive Provider

What is a PowerShell drive provider? PowerShell supports the concept of managing resources as if they were drive volumes. Just as you can CD into a file folder, PowerShell

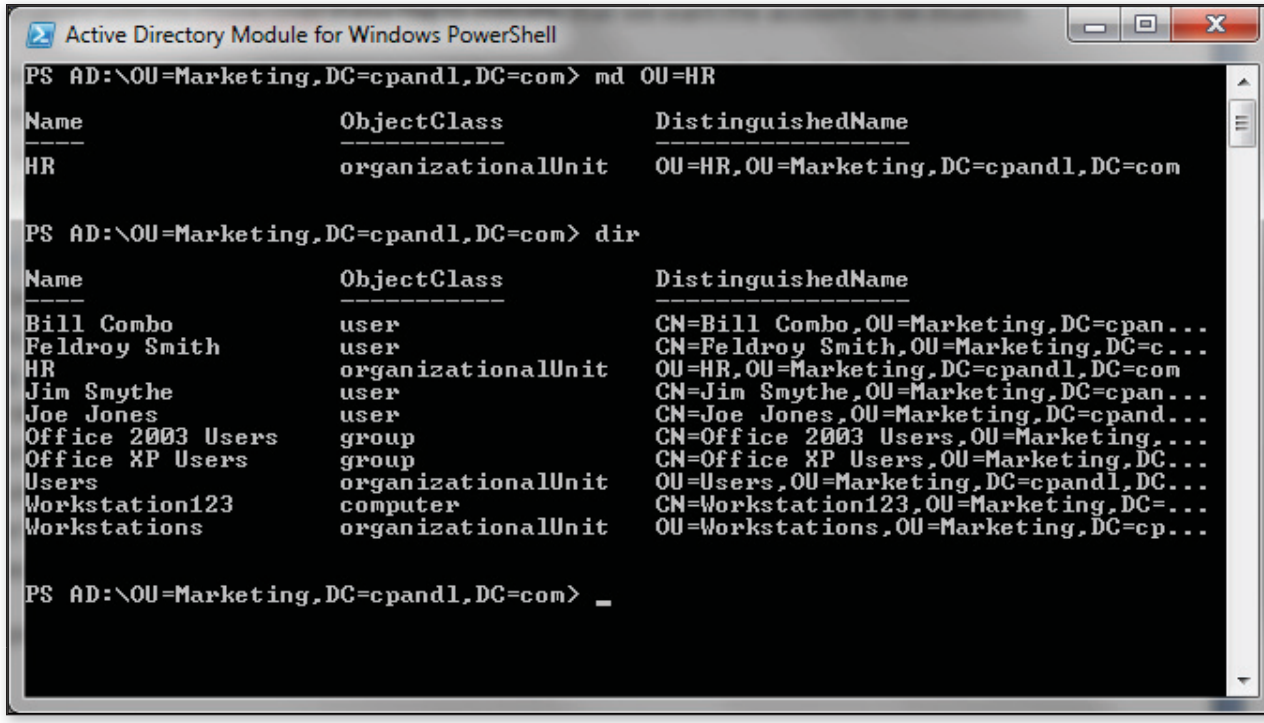


Figure 2: Creating an OU using the PowerShell drive provider

drives let you navigate other types of resources the same way. For example, in PowerShell 1.0, Microsoft provided a registry PowerShell drive so that you could treat registry keys and values as folders and files. You could change directories in PowerShell to HKEY_LOCAL_MACHINE, then navigate through keys, adding and removing keys and values using commands similar to what you would use in the file system. Microsoft has provided a PowerShell drive provider for AD along with the cmdlets. This PowerShell drive lets you treat your AD hierarchy like a file system. To use this feature, open PowerShell with the AD module loaded. Then type:

```
cd AD:
```

The drive prompt changes to reflect the new drive you're working from. If you type DIR from here, you'll get a list of all the partitions within your current AD forest. Suppose you want to navigate into your AD domain and create a new organizational unit (OU). From the top-level AD: drive context, type:

```
cd "DC=cpandl,DC=com"
```

(Replace DC=cpandl,DC=com with your AD domain's directory name.)

Between the cmdlets and the Active Directory provider, you have a whole new set of options for command-line management of Active Directory in Windows 7 and Windows Server 2008 R2.

Now let's say we want to create a new HR OU under the Marketing OU. To change to the Marketing OU folder, type:

```
cd "OU=Marketing"
```

Finally, to create the HR OU under Marketing, type:

```
md "OU=HR"
```

It's as simple as that. Figure 2 shows the output from these commands.

Of course, this example is only the tip of the iceberg when using the AD PowerShell drive. Using this method you can perform most tasks against AD that you can perform within a file system. And, you can include PowerShell drive commands in scripts to further automate AD management.

Streamline AD Management

I've only scratched the surface of what you can do with the new AD capabilities in PowerShell. Between the cmdlets and the AD provider, you have a whole new set of options for command-line management of AD in Windows 7 and Server 2008 R2. I highly recommend you spend time working with this new module to learn how it can help streamline your AD management.

InstantDoc ID 103360

Darren Mar-Elia
(dmarelia@windowsitpro.com) is a contributing editor for *Windows IT Pro* and is CTO and founder of SDM Software (www.sdmsoftware.com). He maintains a Group Policy resource website (www.gpoguy.com) and is coauthor of *Microsoft Windows Group Policy Guide* (Microsoft Press).

Use MSAs to Ease the Pain of Administering Service Accounts

by John Savill

Managed service accounts could be Windows Server 2008 R2's best feature

People are excited about Windows Server 2008 R2 for a lot of reasons, including the AD Recycle Bin, a very welcome capability to cleanly restore objects that have been deleted. But after organizations actually start using Server 2008 R2, another feature they find even more useful is the managed service account. The MSA feature might very well change the way you administer your service accounts and cure a lot of pains your organizations faces related to service accounts.

Why MSAs?

Many services require integration with other network resources and directory services beyond just the local computer, which typically means a service runs as either the built-in Network Service Account, the built-in Local System Account, or a specified domain user account. However, numerous issues arise when using these built-in accounts.

Often services require specific rights and privileges. Using the built-in accounts, especially the Local System Account, means the service has rights and privileges far in excess of what is actually required on the local machine and possibly the network, which increases the chances of security problems.

The problem of excessive privileges with the Local System Account is why the Network Service Account was introduced with Windows Server 2003, as a way to have a built-in account that didn't have full system privileges on the local machine, while still providing network access as the computer account. Beyond the problem of excessive privileges, when many services use the same account it's hard to audit actions performed on the server.

Most applications that require services advise you to create a domain user account for the service and grant a specific set of permissions. Administrators generally try to minimize the number of accounts, and therefore often one domain account is used for multiple services. However, the shared account needs the sum of all required permissions for all the services sharing the account, so each individual service effectively has more permissions than it actually needs.

If you do decide to use a domain user account for each service, the biggest challenge arises: managing the passwords for these domain user accounts. The solution typically falls into one of two camps. Either you set the password on the domain user account to never expire, which is a large security problem that will cause companies to fail most audits, or the passwords expire per normal domain security policy—which in most companies causes outages to the service as the passwords fail to get updated, causing the service to fail until an administrator manually intervenes and resets the password.

No More Password Hell

MSAs address this password management problem by providing automated password regeneration through the netlogon process, the same way the computer account has its password automatically reset. By default, every 30 days the netlogon process generates a new 240 random-character

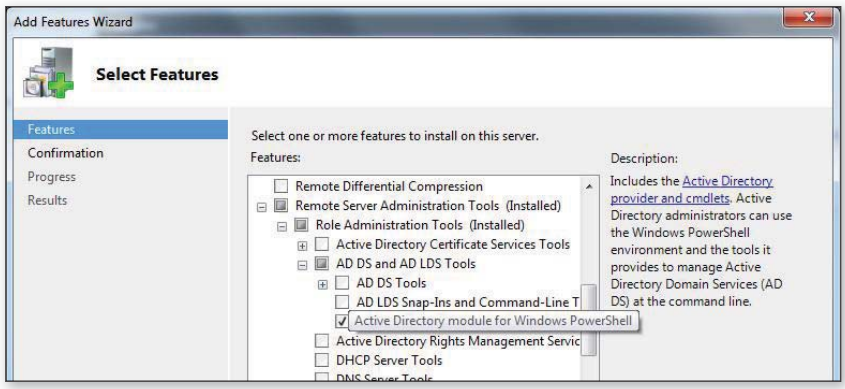


Figure 1: Installing the Active Directory PowerShell cmdlets

password and synchronizes it with the domain. Domain security policies and fine-grained password policies are ignored by computer objects and MSAs, so the password is always 240 characters as opposed to following the guidelines specified in the aforementioned policies, such as eight-character passwords. To use MSAs, two requirements must be met:

1. The AD forest must have been prepared with the Server 2008 R2 forest prep, adding a new object class, msDS-ManagedServiceAccount, which stores information for the MSA in AD.

2. The machine using the MSA must be running Server 2008 R2 or Windows 7. There are currently no plans to back-port the MSA functionality into earlier versions of Windows.

The good news is you don't need to be running in Server 2008 R2 or even Server 2008 domain mode. However, if you're running all Server 2008 R2 domain controllers (DCs), you get an extra piece of functionality with MSAs that I'll cover later.

A new container is created at the root of the domain, Managed Service Accounts, which is the default location of all MSAs, but you can relocate MSAs if you want. To view details about MSAs created in this container, enable the Advanced Features view within Active Directory Users and Computers (ADUC).

However, you can't manage MSAs by using the GUI—as with lots of the goodies in Server 2008 R2 AD, you need to use PowerShell to manage them. This brings us to actually using an MSA. To use an MSA for a service, you need to take four steps:

1. Create the MSA in AD using the New-ADServiceAccount PowerShell cmdlet.

2. Associate the MSA with a specific computer account in AD by using the Add-ADComputerServiceAccount PowerShell cmdlet.

3. Install the MSA on the computer by using the Install-ADServiceAccount PowerShell cmdlet.

4. Configure services on the computer to use the MSA, which can be done through the Microsoft Management Console (MMC) Services snap-in (services.msc) or any other service management interface such as WMI, SC, or PowerShell.

Note that part of this process is to associate the MSA with a specific computer account, which is a restriction of the MSA—the MSA can only be used on a single computer. However, the MSA can be used by multiple services on that computer (though you still shouldn't share accounts because of auditing and excessive permissions reasons), and one computer can have multiple MSAs. Because of the inability to span multiple machines, you can't use the MSA for any purpose that spans multiple machines; for example, you can't use an MSA on cluster nodes nor in any kind of load-balancing that uses Kerberos authentication.

Creating and Using MSAs

Let's dig a bit deeper and actually create an MSA, install it on a server, then configure a service to use the MSA. In all cases in which you run any of the PowerShell cmdlets, you need to have installed the Active Directory Module for Windows PowerShell, which is part of the Remote Server Administration Tools (RSAT) feature and can be found in the Active Directory Domain Services (AD DS) and Active Directory Lightweight Directory Services (AD LDS) Tools section, shown in Figure 1. These cmdlets need to be on both the computer you're managing the MSA from and the servers that are using the MSA.

Next, open a PowerShell window to import the module, called ActiveDirectory, which will enable access to the AD cmdlets. You need to import this anytime you start a new PowerShell instance and want to use the AD cmdlets. To import the module, type

```
Import-Module ActiveDirectory
```

We can now create a new MSA. It's a good idea to have a naming standard for your MSAs. Because they are tied to a specific computer, using the target computer name as part of the name might help. First, I create an MSA named msa_ts01_purgesvc, which I'm going to use on server savdalts01:

```
New-ADServiceAccount -name msa_ts
  01_purgesvc -enabled $true
```

Next, I link the MSA to server savdalts01:

```
Add-ADComputerServiceAccount -identity
  savdalts01 -serviceaccount msa_ts01
  _purgesvc
```

Then I log on to the server that will use the MSA; in my case, savdalts01. After I log on, I make sure I have the AD module for PowerShell installed. Then I start a PowerShell window and import the AD module. I then install the MSA:

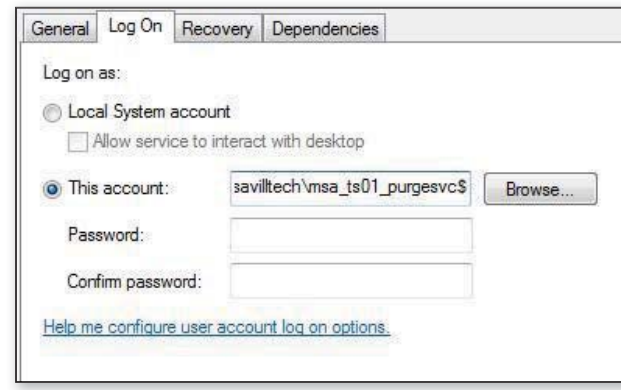


Figure 2: Configuring a service to use the MSA

```
Install-ADServiceAccount -identity
  msa_ts01_purgesvc
```

At this point the account *domain*\msa_ts01_purgesvc$ (e.g., savilltech\msa_ts01_purgesvc) is available for use by any service on the server. Note the dollar sign at the end of the name and the AD domain name at the start.

I use the MMC Services snap-in (services.msc) and enter the name of the MSA and make sure both password fields are blank in the Log On tab, which Figure 2 shows, then start the service. The MSA is now being used, and you won't have to reset a password on it again.

You grant permissions to MSAs and add MSAs to groups just like any other account, and can use Active Directory Users and Computers, and PowerShell cmdlets such as Add-ADGroupMember. To force a reset of the MSA password, use the command

```
Reset-ADServiceAccountPassword -identity
  <MSA name>
```

although this shouldn't be necessary.

If you decide you no longer want to use a specific MSA, you need to update the service(s) using the MSA to log on as an alternate account, then run the command

```
Remove-ADServiceAccount -identity
  <MSA name>
```

to remove the MSA from the server.

Service Principal Name Delegation

MSAs also address another pain of service accounts, Kerberos Service Principal Name (SPN) management. SPNs are registered by services in AD. Clients search by them to find the user or computer account used by the service to facilitate mutual authentication. The SPN is part of either a computer or user object.

Normally, SPNs can be updated only by domain administrators. However, sometimes the service can update the SPN if the service is running as the Local System account. MSAs let you delegate SPN management to service administrators after you enable the MSA for delegation. Use the command

```
Set-ADServiceAccount
  -TrustedForDelegation
  $true -identity <MSA name>
```

which allows delegation and lets the target of delegation manipulate the SPNs for the object. SPN management for MSAs is simpler; however, the domain must be in Server 2008 R2 domain mode, which means all DCs need to be running Server 2008 R2. Assuming you're running in Server 2008 R2 domain mode, you now have automatic SPN updating in the following scenarios (which means no manual updates are required):

- Renaming the computer account
- Changing dnshostname attribute of the computer account
- Changing additionaldnshostname attribute of the computer account
- Changing additionalsamaccountname attribute of the computer account

Virtual Accounts

If access to a specific domain-level account isn't required and the computer's account is what you need, a spin-off of the MSA feature is available. A virtual account acts like a unique instance of the Network Service account on the local computer and lets you avoid using the generic Network Service account and the associated audit problems related to sharing accounts. Because a virtual account acts like a unique clone of the built-in Network Service account, when the service communicates with other resources on the network it does so as the computer object account. You must be a local administrator to configure virtual accounts.

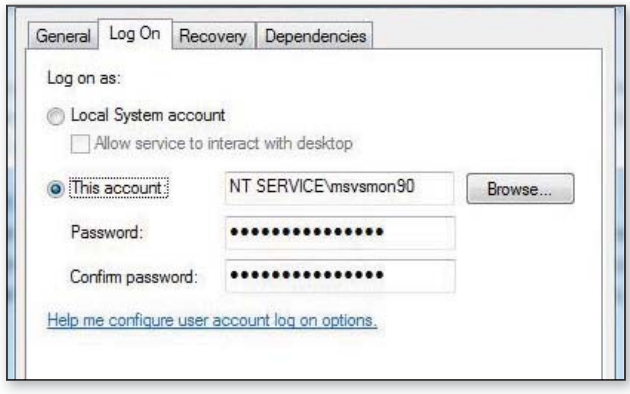


Figure 3: Configuring the Visual Studio remote debugger to use a virtual account

Like MSAs, virtual accounts are available only on Server 2008 R2 and Windows 7 machines; however, there are no domain or schema requirements and you don't create or manage virtual accounts. To use a virtual account, type "NT SERVICE*service name*" in the Log On tab of the service and ensure both password fields are blank.

The service name you type as the account name must match exactly the service name of the service (and not the long display name). In Figure 3, I configured the Visual Studio (VS) remote debugger to use a virtual account by using the account \NT Service\msvsmon90 with blank passwords. When I hit Apply, the password fields are automatically populated. You can get the short name of a service through numerous means: browse HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services; run the SC QUERY command; or the simplest way, just look at the Service name value that's shown in the General tab of a service's properties.

Support MSAs

Some applications ask during installation for the account and password that will be used. In these instances, after the installation, you can modify the service and copy any rights and privileges to the MSA. However, some applications might not allow this, preventing you from using an MSA with that application. Email the application vendor and ask for MSA support in the next version or via a patch.

Many applications and features do support MSAs, including IIS 7.5 application pool identities. I hope in Windows 8 we'll see MSAs support multi-computer scenarios to support cluster and NLB configurations. Regardless, the MSA is still an awesome feature that will ease a lot of pain related to service accounts.

InstantDoc ID 103265

John Savill
(john@savilltech.com) is an advisory architect for EMC's Microsoft consulting practice. He's an MCITP: Enterprise Administrator for Windows Server 2008 and a 10-time MVP. His latest book is *The Complete Guide to Windows Server 2008* (Addison-Wesley).

COVER STORY

Why You Need WINDOWS SERVER 2008 R2

by Michael Otey

Ward Ralston delves into the technical details of the Server 2008 R2 release

Michael Otey, technical director of *Windows IT Pro*, recently asked Ward Ralston, group product manager for Windows Server, to cover some of the aspects of Windows Server 2008 R2 that might make IT pros consider deploying this release sooner rather than later.

Michael Otey: What are the must-have features in Windows Server 2008 R2?

Ward Ralston: Windows Server is an interesting product in that it's a platform technology. It's no one-trick pony. Today there are 17 roles that can be deployed on Windows Server and more than 42 features and role services to complement those roles. And each one of those roles has something new to offer. So your infrastructure needs and how you deploy Windows Server (file server, application server, web server, DNS server, etc.) will determine where your "must-have" features lie. That said, when we think of the major technology investment areas we focus on for R2, we think of our new hypervisor and its ability to Live Migrate virtual machines, its power management and PowerShell capabilities, and its better-together technologies with the Windows 7 client—such as BranchCache and Direct Access.

Michael Otey: What are the new virtualization capabilities?

Ward Ralston: With Windows Server 2008 R2, there are a number of improvements to the hypervisor around scalability, performance, and reliability. First, on the scalability front, we have increased the number of logical processors supported to 64. This will allow Hyper-V Server 2008 R2 to scale the capabilities of the new multi-core systems as they come to market.

On the performance side, we have the ability to leverage technologies in the CPU known as Nested and Extended page tables (Intel and AMD). Known as second-level address translation (SLAT), it allows us to use memory more effectively and reduce the host overhead of running Hyper-V from roughly 8 percent to 2 percent. We also have introduced new networking capabilities in the hypervisor, such as TCP Offloading and Virtual Machine Queues (VMQ), which give us better network performance.

And finally, on the reliability side, we have developed a technology called Clustered Shared Volumes (CSV) that allows multiple hosts in a cluster to talk to the same shared volume. This gives us the ability to perform Live Migrations of virtual machines with no perceived downtime to the end user connected to the VM while it's running.

Michael Otey: Can you clear up some of the confusion about virtualization and licensing?

Ward Ralston: Microsoft has taken a leadership position over the last few years to ensure that licensing for virtual machines is as straightforward as possible. For Standard Edition, you get one license for a virtual guest; each additional virtual guest requires an additional license. For Enterprise Edition, you get four licenses—so every guest over four requires a license. And for Datacenter Edition, which is the preferred operating system for organizations that are looking to virtualize, we offer an unlimited number of virtual guests. No licenses required at all—essentially a virtualization buffet of all-you-can-eat VMs.

Michael Otey: What's new in Active Directory improvements?

Ward Ralston: There are a couple of cool new things going on here. First is the new Active Directory Administrative Center (ADAC). We got our PowerShell team, our AD team, and our User Experience team together to create an intuitive wizard-driven console for AD management based 100 percent on PowerShell.

Another compelling feature for organizations is the AD Recycle Bin. In the past, if an object was accidently deleted from AD, you would have to take the Domain Controller into safe mode and perform an authoritative restore of that object from backup media. This process could potentially take hours and was only as good as the fidelity of your backup. With Windows Server 2008 R2, you can restore deleted objects from the command line without having to do any disaster recovery procedures. As you may suspect, a requirement of this capability is Windows Server 2008 R2 Forest Functionality Mode.

Michael Otey: Have there been any enhancements to Server Core?

Ward Ralston: Server Core is another area where there have been some significant improvements with Windows Server 2008 R2. One of the customer-driven features we added was the ability to run PowerShell and ASP.Net on Server Core. This was a limitation in the past, as we didn't have a componentized version of the .NET framework, which is now part of Server Core.

Another improvement is with the Server Core memory footprint. We have a new R2 feature called trigger-starting of devices and services. This allows us to bring up certain devices and drivers only when needed instead of at install. This reduced the footprint of a base Server Core install even more. The memory footprint in RAM for Server Core has been reduced to less than 100MB, compared to roughly 130MB for Windows Server 2008 and 244MB for Windows Server 2003, which didn't have a Server Core install option.

We got our PowerShell team, our AD team, and our User Experience team together to create an intuitive wizard-driven console for AD management based 100 percent on PowerShell.

Michael Otey: Terminal Services has been renamed to Remote Desktop Services. Why? And what else has changed?

Ward Ralston: Microsoft has been investing in many new remote desktop and Virtual Desktop Infrastructure (VDI) areas with Windows Server 2008 R2. These changes include adding support for VDI scenarios by integrating Terminal Services and VDI management infrastructure, enabling simplified access to desktops and applications, and providing a much improved rich-media user experience. To better reflect the new capabilities to offer desktop and applications in a firewall-friendly manner to users—wherever they may be—we named everything formerly known as Terminal Services to Remote Desktop Services (RDS).

Windows Server 2008 R2 Remote Desktop Services embraces VDI scenarios, delivering a complete business desktop to employees' remote PCs and other access devices—anywhere. The new Remote Desktop Connection Broker, which extends the Session Broker capabilities already found in Windows Server 2008, makes it easier for administrators to deliver remote resources (desktop or applications) to end-user devices.

The Remote Desktop Connection Broker currently supports four key deployment scenarios: session-based remote desktops; session-based remote applications (RemoteApp); VM-based, personal (permanent) virtual desktops; and VM-based, pooled (non-permanent) virtual desktops.

If your organization includes structured task workers, such as call center and retail branch employees, you can provide access to a session-based desktop or to session-based applications installed on a Remote Desktop Session Host. This type of deployment allows access to standard applications in a cost-effective manner and enables users to access line-of-business applications even from their legacy systems.

We think there are many advantages to virtualizing desktops and applications, such as accelerating application deployment and maintenance and simplifying ongoing management. Users access applications in a central location on a virtual desktop, or on a remote desktop session host. Also, virtualizing desktops can help IT pros deploy new applications to a wide variety of clients, including those on which the new application cannot run natively. PC hardware upgrades aren't required to deploy new applications.

Because applications aren't installed locally, Remote Desktop Services enables more streamlined desktop OS images on PCs, accelerating organizations' ability to adopt new operating systems such as

Windows 7 or use thin clients, both of which can lower management costs.

With RDS, desktops and data live in the datacenter, so only encrypted keyboard and mouse strokes transmit over the network. Centralization of data helps to radically simplify the challenges associated with regulatory compliance. And finally, this approach lets IT departments quickly and easily connect remote or mobile workers with the critical applications and secure work environments they need—from the worker's laptop, home computer, or airport kiosk—by accessing a secure web page to launch applications and virtual desktops that aren't installed or available on the client machine.

Michael Otey: Are there any features in Windows Server 2008 R2 that are important but easy to overlook?

Ward Ralston: Thinking back to the first question—Windows Server is a platform technology. There is a little something for everyone, depending on the roles you deploy it for. For example, a powerful technology in the DNS server role is DNS Security (DNSSEC), which gives you the ability to ensure DNS lookups are served from a trusted source. Or, from a management perspective, Server Manager now has the ability to connect remotely to other servers for administration. The File Server role now has the new File Classification Infrastructure (FCI), which allows you to classify files based on the business value and take action on those files—for example, moving all files that contain the word string "Company Confidential" to an encrypted folder.

One set of features that stands out more than others, though, is our power management capabilities. From throttling the voltage applied to CPUs through the new Power Process Management (PPM), to turning off unneeded cores with Core Parking, to monitoring the wattage of your power supplies—there is a lot of potential to save money on your power bill with R2.

Michael Otey: What are some of the benefits that you get by running Windows Server 2008 R2 and Windows 7 together?

Ward Ralston: As a joint development effort from the beginning, one of the goals of Windows Server 2008 R2 and Windows 7 was to enable users to access the information that they need, whether they are in or out of the office, and in the case of Branch Offices, accelerate the delivery of that information and decrease WAN usage.

One of the challenges we've heard users have today when accessing resources that are inside the corporate network is establishing a VPN. VPN can be hard to use for users because it takes time and multiple steps to initiate the VPN connection and wait for the PC to be authenticated from the network. And if you're lucky, the L2TP/PPTP ports will be open on the firewall from the location you are connecting from. Hence, most remote users try to avoid the VPN as much as possible and stay disconnected from the corporate network for as long as they can. At this point, we run into a chicken-egg problem: Since remote users are disconnected, IT cannot manage them while away from work. Remote users stay more out of date and it gets harder and harder to access corporate resources.

With the capabilities that R2 enables, users who have Internet access will be automatically connected to their corporate network without any user interaction—it's just on. A user who is sitting in a coffee shop can open his laptop, connect to the Internet using the wireless access of the coffee shop, and start working as if he's in the office. The user in this case will be able to not only use Outlook, but also work with intranet sites, open corporate shares, use line-of-business applications, and basically have full access to corporate resources.

This solution is also very appealing to IT pros as well—managing mobile PCs has always been an issue since they could be disconnected from the corporate network for a long time. With this work access solution, as long as they have Internet connectivity, users will be on the corporate network. Servicing mobile users (such as distributing updates and Group Policy) is easier since mobile devices can be accessed more frequently by IT systems.

Another area in which Windows Server 2008 R2 and Windows 7 shine is in the branch office. A new feature, BranchCache, is easily enabled using Group Policy. When enabled, R2 will intelligently cache data the first time it is downloaded from a corporate content server (either SMB or HTTP) so that subsequent requests for the same information are served up locally in the branch instead of taxing the WAN links. This is done in a way where we can ensure file changes, ACLs, file locks, etc. are all respected. Think of a branch where there are 100 users who all need to download the new employee manual, which is 50MB. Instead of 5GB going across the WAN in the early morning (slowly), only 50MB will go across and everyone will get the manual locally from the hosted cache in the branch. You just saved 4.5GB on that line.

Michael Otey: What's the upgrade path for earlier versions of Windows Server?

Ward Ralston: People moving from Windows Server 2003 or Windows Server 2008 should have a fairly straightforward upgrade. Although we find most of our customers don't upgrade, but rather migrate with new server hardware, you should still keep these steps in mind.

First, check with your ISV to ensure your applications are tested for compatibility. For a quick compatibility self-test check, you can take advantage of our free downloadable certification toolkit (use the Works with Windows Server 2008 R2 tool) as a black-box validation tool for application compatibility compliance verification. (You can find the Toolkit at microsoft.com/windowsserver/isv). If your ISV has not pledged support for Windows Server 2008 R2 (you may find a complete list of server pledged supported apps on our WindowsServerCatalog.com), we have application compatibility resources including the Microsoft Deployment Toolkit 2010 (MDT), which has the Application Compatibility Toolkit 5.5 (ACT).

Second, remember that Windows Server 2008 R2 is x64 only. You can't upgrade from an x86 operating system to an x64 because the architectures are different. Also, keep in mind that WoW64 (Windows-on-Windows 64-bit) is capable of running 32-bit apps on a 64-bit OS. Third, check out the MDT as your first step in assessing your upgrade, migration, or new deployments of Windows Server 2008 and Windows Server 2008 R2.

InstantDoc ID 103298

CUTTING-EDGE CONTENT • EXPERT SPEAKERS • GREAT LOCATION

SharePoint Pro
2010 SUMMIT & EXPO

MARCH 16-19, 2010 • LAS VEGAS

Celebrate the Upcoming Release of SharePoint 2010
with your colleagues & attend exciting in-depth sessions delivered by Microsoft & industry experts.

Book 3 nights by January 22, 2010 at the Bellagio Hotel and receive $100 Bellagio certificate.
Book NOW to get a special rate of $149 (a limited number of rooms at this rate, so reserve today).

Thomas Rizzo
Microsoft

Steve Fox
Microsoft

Andrew Connell
Critical Path Training, LLC

Dan Holme
Intelliem, Inc.

Scot Hillier
Scot Hillier Technical Solutions, LLC

- Dive into SharePoint 2010 with industry experts
- Get the insiders scoop at cutting-edge Microsoft keynotes
- Explore the best migration path to SharePoint 2010
- Expand your social network and build valuable relationships
- Visit the expo hall for new products and services

www.SharePointProSummit.com

203-400-6121 OR CALL TOLL FREE AT **800-438-6720**

Microsoft® DevConnections magazine SharePoint Pro CONNECTIONS TECH Conferences Inc. PENTON MEDIA

SharePoint Pro 2010 SUMMIT & EXPO

The Top Reasons to Attend

- Celebrate the upcoming release of Sharepoint 2010 with members of the teams that built the products.
- Find out from industry insiders the best migration path if your company is considering an upgrade.
- Listen to Microsoft discuss the many enhancements and new features of SharePoint 2010.
- Find products and services from our partners in the Expo Hall that can save money, save time, and help your business do more.
- Book your hotel early and take advantage of GREAT hotel rates at the world famous Bellagio. Reserve your room at the Bellagio by the early bird date and get a $100 Bellagio certificate.
- A strong network of peers is an invaluable resource; build yours with the unparalleled networking opportunities at the conference. Come prepared to meet and interact with people at other companies and take advantage of their experiences.
- Unwind in Vegas and make new friends! You know what they say about Vegas…
- Impress your boss and colleagues. You'll go back to the office with practical tips and tricks that will make development, deployment, and administration of your SharePoint solutions faster and easier.
- Enjoy the excitement and luxury of one of Las Vegas' premiere hotels. Enjoy some of the best dining in the culinary world, famous Vegas shows, fine shopping, the famous fountains of the Bellagio, the gallery of fine art, the World-famous Shadow Creek golf course and the 24/7 buzz of the casino.

SCHEDULE at a Glance

TUESDAY, MARCH 16, 2010	
7:30 am - 5:00 pm	Conference Registration
9:00am - 4:00 pm	Pre-conference Workshops
WEDNESDAY, MARCH 17, 2010 MICROSOFT DAY	
7:30 am - 5:00 pm	Conference Registration
7:30 am - 8:30 am	Continental Breakfast
8:00 am - 9:00 am	Keynote
9:30 am - 11:30 am	Conference Sessions
11:30 am - 1:00 pm	Lunch
1:00 pm - 4:00 pm	Conference Sessions
8:30 am - 5:00 pm	Expo Hall Open
THURSDAY, MARCH 18, 2010	
7:30 am - 5:00 pm	Conference Registration
7:30 am - 8:30 am	Continental Breakfast
8:30 am - 11:30 am	Conference Sessions
11:30 am - 1:00 pm	Lunch
1:00 pm - 4:00 pm	Conference Sessions
8:30 am - 4:00 pm	Expo Hall Open
FRIDAY, MARCH 19, 2010	
7:00 am - 8:00 am	Continental Breakfast
8:00 am - 11:30 am	Conference Sessions

Microsoft Day

SAMPLING OF SESSIONS PRESENTED BY MICROSOFT SPEAKERS.

Please check Web site as we add more sessions that are currently under NDA.

DEVELOPER

HMS01: OVERVIEW OF MICROSOFT SHAREPOINT 2010 FOR THE DEVELOPER
MICROSOFT

HMS02: INTRODUCTION TO SHAREPOINT DEVELOPMENT WITH VISUAL STUDIO 2010
MICROSOFT

HMS03: DEVELOPING BUSINESS INTELLIGENCE SOLUTIONS WITH SHAREPOINT 2010
MICROSOFT

HMS04: DEVELOPING INTERNET-FACING SITES USING SHAREPOINT 2010
MICROSOFT

HMS05: ENHANCING THE SHAREPOINT 2010 USER EXPERIENCE THROUGH SILVERLIGHT
MICROSOFT

HMS06: DEVELOPING ENTERPRISE APPLICATIONS USING THE BUSINESS CONNECTIVITY SERVICES
MICROSOFT

HMS07: EXTENDING THE ENTERPRISE SEARCH EXPERIENCE IN SHAREPOINT 2010
MICROSOFT

IT PRO

HMS08: UPGRADING FROM SHAREPOINT 2007 TO SHAREPOINT 2010
MICROSOFT

HMS09: OVERVIEW OF ENTERPRISE CONTENT MANAGEMENT IN SHAREPOINT 2010
MICROSOFT

HMS10: TOP TEN SHAREPOINT 2010 FEATURES FOR THE IT PROFESSIONAL
MICROSOFT

HMS11: OVERVIEW OF HOW TO DEPLOY SOLUTIONS TO SHAREPOINT SERVER 2010
MICROSOFT

HMS12: INTRODUCTION TO SHAREPOINT 2010 ADMINISTRATION
MICROSOFT

HMS13: WHAT'S NEW FOR SECURITY IN SHAREPOINT 2010
MICROSOFT

SHAREPOINT DEVELOPMENT

HDEV01: UPGRADING AND EXTENDING SHAREPOINT 2007 WCM SITES WITH SHAREPOINT SERVER 2010 WEB CONTENT MANAGEMENT
ANDREW CONNELL

In this session, you'll see how to upgrade a SharePoint 2007 WCM site to SharePoint Server 2010 WCM and leverage some of the new capabilities. After upgrading the site, you'll learn how to implement the ribbon and convert to the new SharePoint 2010 UI visuals. Next you'll see how to add ratings and use the content organizer.

HDEV02: INTERACTING WITH SHAREPOINT 2010 OFF THE SERVER: INTRODUCING THE CLIENT OBJECT MODEL
ANDREW CONNELL

This session demonstrates client object model, new to SharePoint 2010. This addition makes it much easier for developers to create custom solutions that leverage data stored in SharePoint from off the SharePoint server with a familiar API and without traditional Web Services. Topics covered include the .NET and Silverlight managed client object models as well as the ECMAScript object model.

HDEV03: CUSTOMIZING SHAREPOINT 2010 ENTERPRISE CONTENT MANAGEMENT DOCUMENT SETS
ANDREW CONNELL

SharePoint Server 2010 Enterprise Content Management (ECM) introduces a new concept called document sets. These enable you to create a single work product made up of multiple components. In this session, you'll learn how to create customizable document sets, custom welcome pages and much more!

HDEV04: INTRODUCTION TO SHAREPOINT DESIGNER 2010: TOP 5 GREAT THINGS TO KNOW!
ASIF REHMANI

SharePoint Designer 2010, which is a free application, is "The Preferred" tool to design powerful no-code solutions and applications in SharePoint 2010. In this session, you will get a broad overview of the capabilities of the tool, from site customizations such as modifying Site Metadata, managing Site Security, or creating Site Content, to building List- or Site-based Workflows and connecting to a variety of data sources. You will also learn about the new ribbon interface of SharePoint Designer 2010 and you'll see how best to take advantage of this application by showing the new bells and whistles that come with this product.

HDEV05: OVERVIEW: CREATING WORKFLOWS WITH SHAREPOINT DESIGNER 2010, INFOPATH AND VISIO
ASIF REHMANI

Forms and workflows are important for automating business processes. Companies usually rely on programmers to create the forms and workflows using code. Not anymore! With InfoPath 2010 and SharePoint Designer 2010, you can create powerful data-driven form composite solutions on your SharePoint sites. InfoPath gives you the ability to pull data from databases and lists, and create forms with data validation and conditional formatting. SharePoint Designer's workflows let you then design powerful multi-step workflows centered around the form collected data, building upon the out-of-the-box reusable workflows and even import workflow designs from Visio! In this session, you will see how these tools come together to design powerful end-to-end solutions on your sites.

HDEV06: GENERATE AND PUBLISH ELECTRONIC FORMS ON YOUR INTRANET USING INFOPATH 2010... NO CODE REQUIRED!
ASIF REHMANI

Finally, you can make your goals of going paperless a reality! Microsoft Office InfoPath 2010 and Forms Server 2010 come together to provide a powerful platform for electronic form generation. In this session, you will see how you can build robust electronic forms with data validation and conditional logic rules using InfoPath. Also, the inherent power of InfoPath will be demonstrated to look up data from various sources and populate it in your custom designed electronic forms. All this and more will be accomplished without writing a single line of code!

HDEV07: INDUSTRIAL STRENGTH RECORDS MANAGEMENT IN SHAREPOINT 2010
JOHN HOLLIDAY

SharePoint 2010 introduces several new document management and records management features which together represent the next generation of records management capabilities that were previously available only in the SharePoint 2007 Records Center. In this session, we'll examine document sets, persistent document identifiers, metadata-driven routing and the content organizer and we'll explore ways to apply these new features to solve traditional records management problems such as electronic record authentication and the deployment of integrated data integrity controls. During the session, we'll explore the new in-place records management features that make it easier to manage document retention schedules. You'll learn how to use con-

Sessions and speakers are subject to change. Check the Web site for details.

tent organizer rules to create detailed plans for managing how official records are organized within a given site. We'll also explore the new and improved SharePoint 2010 information management policy architecture, which includes both location-based and multiple-stage information policies, and we'll take a detailed look at the improved records center site definition to see how it simplifies the creation of a locked-down records vault.

HDEV08: PROGRAMMING BUSINESS CONNECTIVITY SERVICES SOLUTIONS IN OFFICE 2010

JOHN HOLLIDAY

SharePoint 2010 Business Connectivity Services (BCS) represents a major step in the evolution of the Business Data Catalog, with richer functionality that includes the ability to create and update back-end data, and much tighter integration with Office client applications. These new capabilities are exposed through a rich set of enhancements on both the client and the server. In this session, we'll examine both code and no-code approaches to building BCS solutions in Office 2010. First, we'll explore the new SharePoint 2010 integration features provided by the Visual Studio 2010 Tools for Office Development. Then we'll take a look at what it takes to build BCS Declarative Solutions that require no coding. During the session, we'll use the BDC client-side API to build a VSTO 4.0 add-in that integrates Line of Business (LOB) data with Microsoft Office client applications via SharePoint 2010 External Content Types and Lists.

HDEV09: EXTENDING THE VISUAL STUDIO 2010 SHAREPOINT TOOLS

TED PATTISON

The introduction of the Visual Studio 2010 SharePoint Tools really raises the bar in terms of developer convenience and productivity. And while the out-of-the-box experience with these tools goes far beyond what's been available to SharePoint developers in the past, the SharePoint Tools have been designed from the ground up to support extensibility. This session shows you how to get started by explaining how to extend the SharePoint Project System and how to use the extensibility APIs. You will learn how to create custom templates for SharePoint Projects and SharePoint Project Items (SPIs) to support common scenarios such as a solution for deploying a custom master page along with its own CCS and JavaScript files. You will also see how to extend SPIs with custom properties, context menus and event handlers.

HDEV10: SECURITY CHANGES AND ENHANCEMENTS IN SHAREPOINT 2010

TED PATTISON

SharePoint 2010 introduces a new claims-based security model that will impact the way the companies design, implement and enforce security with their SharePoint sites. This session explains the fundamental concepts of a claims-based model and shows how the new claims-based model makes it possible to use new types of security principals such as Active Directory distribution lists and SharePoint Server Audiences as first-class security objects which can be used to securely configure access to securable objects such as sites, lists, items and documents. The session will walk through developing a custom claims provider with Visual Studio 2010, which will effectively demonstrate the flexibility of how we define the people and groups from whom you need to configure access.

HDEV11: BEST PRACTICES FOR ACCESSING SHAREPOINT 2010 LIST DATA

SCOT HILLIER

In this session, attendees will learn the best ways to access and manipulate list data in SharePoint 2010. This session will begin with a discussion of server-side access using LINQ including the use of SPMetal for entity generation, writing LINQ queries against lists, and joining lists. Next, the session will present client-side access using ADO.NET Data Services through the ListData.svc service. Coverage will include using a Windows Presentation Foundation (WPF) client and a Silverlight 3.0 client. Attendees will exit the session with a strong understanding of how to utilize list data in their applications.

HDEV12: USING BUSINESS CONNECTIVITY SERVICES TO ACCESS EXTERNAL SYSTEMS WITH SHAREPOINT 2010

SCOT HILLIER

Business Connectivity Services (BCS) can be thought of as the next evolution of the Business Data Catalog (BDC) that provides a read-write capability to external data. In this session, we will cover the fundamental concepts and tools necessary to use BCS in SharePoint solutions. The session will begin by presenting the concept of an external content type (ECT) and showing how to create them in the SharePoint Designer. The ECTs will then be used to create external lists that act as a front end for a data source. Finally, attendees will learn to create a .NET Assembly Connector, which allows the creation of custom solutions for accessing external data within the BCS framework. Attendees will exit the session with a strong understanding of the BCS architecture, tools, and development practices.

HDEV13: CREATING SEARCH-BASED SOLUTIONS WITH SHAREPOINT 2010

SCOT HILLIER

Search-based solutions are applications that use a search page as the primary interface. Solutions such as image searching or travel searching in Bing are good examples of search-based solutions. SharePoint 2010 offers developers new ways to extend search and create search-based solutions. In this session, attendees will learn to create search-based solutions by using custom relevance models, extending SharePoint 2010 search parts, and utilizing .NET Assembly Connectors to access external systems. The techniques presented will prepare attendees to create search-based solutions on their own.

HDEV14: CREATING CUSTOM OFFICE BUSINESS APPLICATIONS WITH BUSINESS CONNECTIVITY SERVICES AND THE SHAREPOINT CLIENT OBJECT MODEL

TODD BAGINSKI

This session demonstrates how to build rich Office business applications which connect to data sources through the BCS and the SharePoint Client Object Model. First, the session demonstrates how to register a data source with the BCS which pulls data from multiple data sources. Then the session shows how to use the SharePoint Client Object Model to display and update the data within Microsoft Office applications. Finally, the session will demonstrate how to enhance your Office business applications even further with data stored in SharePoint lists and libraries and the SharePoint Search Service. Whether you are looking for in-depth technical knowledge about these components, or just want to get some ideas how Office business applications may be used to streamline processes and save time in your organization, this is the right session for you.

CHECK WEB SITE AS WE CONTINUE TO ADD MORE SESSIONS, SPEAKERS AND MAKE UPDATES

www.SharePointProSummit.com

HDEV15: HOW TO CREATE A YOUTUBE-LIKE APPLICATION IN SHAREPOINT WITH THE DIGITAL ASSETS LIBRARY–WITHOUT WRITING ANY MANAGED CODE!

TODD BAGINSKI

This session demonstrates how to use the new Digital Assets Library and the Videos content type to create YouTube-like functionality in your SharePoint sites. First, the session describes the new functionality the Digital Assets Library provides for videos, images, and audio files. Then the session shows how to create and configure the Digital Assets Library to display a list of videos complete with thumbnail previews. Finally, the session shows how to create a page to watch each video inside a Silverlight video player and display the details about it. All of this great functionality is implemented without writing a single line of managed code; only JavaScript, HTML, and CSS are needed to deliver the functionality!

HDEV16: SHAREPOINT 2010 DEVELOPER BEST PRACTICES

KIRK EVANS

This session will focus on best practices for developing with SharePoint 2010, including configuring a development environment, configuring application lifecycle management, unit testing, and understanding defensive development techniques.

HDEV17: DEVELOPING ADVANCED SHAREPOINT 2010 WORKFLOWS WITH VISUAL STUDIO 2010

KIRK EVANS

SharePoint 2010 includes a number of new facilities for workflow developers. Come to this session to hear about what's new in SharePoint 2010 and Visual Studio 2010 to help you code, deploy, and debug workflow solutions.

HDEV18: APPLICATION LIFECYCLE MANAGEMENT WITH SHAREPOINT 2010 AND TEAM FOUNDATION SERVER 2010

KIRK EVANS

A key part of developing for SharePoint 2010 is understanding how to work within a team of developers effectively. This requires a structured application lifecycle management process including centralized source code and build management. Come to this session to understand how to get more out of Team Foundation Server 2010 while building SharePoint 2010 solutions.

SHAREPOINT ADMINISTRATION

HITP01: DESIGNING GOVERNANCE: HOW INFORMATION MANAGEMENT AND SECURITY MUST DRIVE YOUR DESIGN

DAN HOLME

You've read the white papers, you've "Binged" governance, but how, exactly, do you design a SharePoint implementation that will support governance, security, and information management? Join SharePoint MVP and consultant Dan Holme for a practical, nuts-and-bolts look at the close relationship between your information management requirements and SharePoint's manageability controls, and the demands that relationship places on your design and infrastructure. This session is focused on architecting a logical design of SharePoint that effectively supports your information management requirements and governance plan–the "technical" side of governance. You will learn how to align your governance requirements with SharePoint farms, Web applications, and site collections. You'll discover why some third-party applications are a "design poison pill" and what SharePoint 2010 offers to greatly improve the deployment of a governable design. Gain a deeper understanding of the intricacies and challenges of designing the logical structure of SharePoint, and take away practical, blueprint-like guidance to what a governed SharePoint implementation might look like in your enterprise.

HITP02: SHAREPOINT TAKES THE GOLD IN TORINO, BEIJING AND VANCOUVER BROADCASTS

DAN HOLME

SharePoint has "won the gold" as a platform for rich collaboration and rapidly deployed solutions during the broadcast of the Olympics from Torino, Beijing and for the upcoming Vancouver 2010. Join Dan Holme, Microsoft Technologies Consultant for NBC Olympics, for an inside look at how SharePoint is put to use in one of the most unique IT efforts in the world. Discover ways that you might leverage SharePoint in your enterprise, and how the Olympics broadcast can inform the choices you make supporting and developing for SharePoint. This unique session sheds an exciting and practical light on the business value and ROI of SharePoint. Ever wonder how you can make the most of SharePoint in your organization? This session might help you figure it out!

HITP03: ENTERPRISE SOCIAL COMPUTING WITH SHAREPOINT 2010

MATTHEW MCDERMOTT

SharePoint 2010 introduces new features that support social computing for organizations of all types. Whether you have a "formal vision" or loose idea of what "social" means to your organization, this session will introduce you to the key concepts and features that can aid in your planning and implementation of social computing for your organization. This session will highlight how companies gain value out of the social computing capabilities of SharePoint.

- Introduction to the "social vision" for SharePoint 2010
- What do I like: Tagging, Rating and Notes
- What's happening: Activity Feeds
- Where is it: Social search
- Who can help: People and Expertise search

HITP04: SHAREPOINT 2010 SEARCH OVERVIEW

MATTHEW MCDERMOTT

Search has taken a huge step forward with the introduction of SharePoint 2010. This session will focus on what is new to Search in SharePoint 2010. Presented through demonstrations of the search capabilities and advancements, this presentation will provide the background necessary to understand how search has improved and how to plan for the smooth implementation of SharePoint search for your organization.

- SharePoint 2010 Search scalability options
- Improved user experience
- Social and people search
- Improved metadata processing
- Improved management and tuning

HITP05: SHAREPOINT MULTILINGUAL SCENARIOS

MATTHEW MCDERMOTT

SharePoint 2010 supports several multilingual scenarios out of the box. This session will detail the features of SharePoint 2010 that enable the creation of publishing sites that support multiple languages and locales. This session will also detail how content contributors can use the new multilingual user interface to work within their chosen language to author, manage and publish content through an interface that supports their native language. This session will detail:

- Planning a multilingual publishing site
- Implementing the multilingual user interface
- The configuration and process required for Variations
- Application of language packs
- Developer considerations for multilingual sites

HITP06: ARCHITECTING A HIGH PERFORMANCE AND FAULT TOLERANT SHAREPOINT 2010 FARM

MICHAEL NOEL

SharePoint server architecture has been significantly improved with the SharePoint 2010 wave. Gone is the inflexible Shared Services Provider, replaced by a much more scalable and fault tolerant architecture. To provide for this level of scalability, a larger number of databases and a certain level of complexity was introduced that should be understood by SharePoint architects before beginning a production SharePoint 2010 deployment. This session delves into the specifics of those infrastructure changes and demystifies many of the concepts surrounding SharePoint 2010 architecture. Best practice architectural scenarios and diagrams are illustrated and compared, and high availability options are discussed in detail.

- Learn how to architect a SharePoint 2010 for High Performance and Fault Tolerance.
- Compare and contrast best practice design examples for SharePoint deployments of varying sizes.
- Understand how to design SharePoint 2010 the right way the first time.

HITP07: BACKUP AND RESTORE FOR SHAREPOINT 2010: PROTECTING MISSION CRITICAL SHAREPOINT DATA WITH NEW TOOLS AND TECHNOLOGIES

MICHAEL NOEL

As more and more organizations use SharePoint to store documents and other critical data, it becomes imperative to provide for backup and restore specific for SharePoint. While some integrated tools exist to provide for disaster recovery, document-level restore capabilities are often needed in a SharePoint environment. This session covers some of those technologies, and focuses specifically on how the new Microsoft System Center Data Protection Manager (DPM) 2010 product can be used to provide for SharePoint-specific backup and item-level restore. In addition, specifics on how to integrate DPM with a SharePoint 2010 farm are provided and best practice architectural examples for DPM, snapshot guidelines, and deployment tips and tricks from the field are covered.

- Explore the new built in backup processes and tools in SharePoint 2010 and what should be backed up.
- Examine item-level recovery capabilities for SharePoint included in System Center Data Protection Manager.
- Learn best practice tips and tricks for deployment of DPM in a SharePoint environment.

HITP08: CONFIGURING SHAREPOINT 2010 FOR EXTRANETS

MICHAEL NOEL

SharePoint 2010 has been specifically designed to provide for a scalable and customizable environment for extranets. Infrastructure changes such as Server Groups, the services architecture, and claims-based authentication have opened the door to external deployment scenarios that were challenging with previous versions of SharePoint. This session covers extranet deployment with SharePoint 2010, focusing on alternate authentication mechanisms, scalability, and security of extranet deployments.

- Learn how to deploy extranets with SharePoint 2010 using a best practice approach to infrastructure design.
- Determine how to use claims-based authentication with SharePoint 2010 for multiple authentication sources.
- Identify how to scale SharePoint 2010 for extranet deployments.

HITP09: PROTECTING YOUR SHAREPOINT 2010 CONTENT WITH SQL SERVER 2008 TRANSPARENT DATABASE ENCRYPTION

MICHAEL NOEL

One of the "killer apps" with SQL Server 2008 is the ability to transparently encrypt all of your SharePoint content databases at the SQL level, without the need to modify any settings in the SharePoint farm. This type of transparent encryption allows organizations to comply with governmental and industry regulations that require content to be stored in encrypted format, but doesn't introduce any new complexities to a SharePoint environment, as the application itself is unaware that any encryption is happening. This session focuses on the best practices, tips and tricks, and real-world advice on how to set up and deploy SQL Server 2008 transparent database encryption for a SharePoint 2010 farm.

- Learn how to set up SQL Server 2008 for transparent encryption of content databases.
- Examine limitations, best practices, and deployment tips for implementing this new capability.
- Take an in-depth look at the security precautions and advice for the encryption methods that can be used and what makes sense for SharePoint.

HITP10: SHAREPOINT SITE LIFECYCLE–CREATING AND ARCHIVING SITES

ROBERT L. BOGUE

Managing information architecture and limiting organic site growth is a difficult issue organizations face. Determining an effective site provisioning and clean up approach that balances end-user control with effective information management for the organization is essential. This session shows developers how to create a flexible solution that lets users get sites up and running quickly, while maintaining stewardship for corporate resource concerns by providing site creation approval, site archiving and site removal strategies. In this session you'll see how to leverage Microsoft InfoPath as a site request form coupled with a SharePoint workflow to approve and create a site. You'll also see the use of new site-level workflows and auditing to monitor the use of the site and recommend when it's time to archive or delete it based upon usage.

HITP11: PROTECTING YOUR SHAREPOINT ENVIRONMENT FROM THE EVIL DEVELOPERS–QUOTAS, SANDBOXES, AND QUERIES

ROBERT L. BOGUE

Whether you believe your developers are evil or just under informed, SharePoint 2010 has a set of tools for you to use to protect yourself from a developer breaking your entire farm. In this session you'll get an IT Pro's introduction to the SharePoint Sandbox and how it can help you including code isolation and execution quotas. You'll also learn about protection from long running queries, and how you can put the pieces together to keep your farm running no matter what the developers throw at it.

HITP12: SHAREPOINT SOLUTION CREATION TOOLS FOR THE IT PRO WITHOUT SEMICOLONS

ROBERT L. BOGUE

Many organizations are struggling to get the support they need. The IT Pro is being asked to help create solutions for business units. The Office System including SharePoint, Visio, InfoPath, Word, and SharePoint Designer are tools that the IT Professional can use to create solutions that don't require a single semicolon. In this very practical session, we'll create a few solutions that every IT Pro can create that will look like you stayed up all night to learn a new (foreign) language.

HITP13: BEGINNING YOUR ADMINISTRATIVE JOURNEY WITH SHAREPOINT 2010

SHANE YOUNG & TODD KLINDT

Time to start talking install and deployment. What are these new things like Prereq installer, farm passphrase, managed accounts, Farm configuration wizard, and pretty icons in central admin? If these are your questions we have your answers. Even if they aren't your questions, swing by. We promise you'll learn something, or at least hear a bad cow joke or two.

HITP14: CONTINUING YOUR ADMINISTRATIVE JOURNEY WITH SHAREPOINT 2010

SHANE YOUNG & TODD KLINDT

Now your farm is running like a well-oiled machine time to look at the new tools. Things like PowerShell, monitoring, backup and restore, performance and large list throttling, and a few other fun things. So many new admin tools and so little time.

HITP15: ADMINISTRATION OF SHAREPOINT 2010 USING POWERSHELL, THE NEW COOLNESS

SHANE YOUNG & TODD KLINDT

All your friends are doing it why aren't you? Stsadm.exe is so 2007. Come to this session to figure out why you need to be a PowerShell guru ASAP and how to amaze your friends and confound your enemies with your new PowerShell skills.

HITP16: SHAREPOINT 2010 ADMINS AND THE DBA DUTIES THEY HATE

SHANE YOUNG & TODD KLINDT

Nobody likes it but it is a fact of life–SharePoint stores everything in SQL Server. Do you know where the most common performance bottleneck for SharePoint is? Your SQL Server. Yikes! So with that being the case, any good SharePoint Admin needs to be up to speed on core SQL Server management. In this session we'll demystify how SharePoint uses SQL, and show what maintenance steps you can take to keep SQL from taking its ball and going home.

HITP17: BETTER TOGETHER: SHAREPOINT, EXCEL, AND ACCESS DELIVER "BIG WIN" SOLUTIONS AND ADOPTION

DAN HOLME

In every organization, mission-critical business intelligence and processes center around Excel worksheets, Access databases, and e-mail-based communications. In this "Better Together" session, you'll learn how to elevate these using out-of-the-box functionality in combinations that achieve "big wins" and drive the success and adoption of SharePoint and Office in your enterprise. This session presents practical, real-world examples to inspire you to identify and solve business problems with SharePoint, Excel, and Access. Decision makers and even power-users will come away armed with an understanding of what amazing things SharePoint and Office can do, together, to deliver high-value solutions, and IT Pros will learn how to guide, implement, configure, and support such solutions. You'll discover approaches for integrating SharePoint, Excel, Access, workflows, Office Web Applications, and more. You'll also learn which solutions can be attained with previous versions of Office and with only SharePoint Foundation/Windows SharePoint Services, and which require SharePoint Server and Office 2010. Technical takeaways include:

- Move important, shared, or multi-user databases from their 20th century home in Excel worksheets and Access databases to SharePoint.
- Create rich, code-free "business intelligence lite" SharePoint solutions that apply SharePoint security and collaboration in unique ways and leverage Excel as an analysis and presentation tool.
- Develop sophisticated, intelligent relational database applications with gorgeous forms and reports using Access as a SharePoint front-end.
- Leverage the new and improved Excel Services and Access Services for high-value, low-effort database solutions.

ALSO:

GENERATE AND PUBLISH ELECTRONIC FORMS ON YOUR INTRANET USING INFOPATH 2010... NO CODE REQUIRED

ASIF REHMANI

Finally, you can make your goals of going paperless a reality! Microsoft Office InfoPath 2010 and Forms Server 2010 come together to provide a powerful platform for electronic form generation. In this session, you will see how you can build robust electronic forms with data validation and conditional logic rules using InfoPath. Also, the inherent power of InfoPath will be demonstrated to look up data from various sources and populate it in your custom designed electronic forms. All this and more will be accomplished without writing a single line of code!

SHAREPOINT DESIGNER 2010: TOP 5 GREAT THINGS TO KNOW!

ASIF REHMANI

SharePoint Designer 2010, which is a free application, is "The Preferred" tool to design powerful no-code solutions and applications in SharePoint 2010. In this session, you will get a broad overview of the capabilities of the tool, from site customizations such as modifying Site Metadata, managing Site Security, or creating Site Content, to building List- or Site-based Workflows and connecting to a variety of data sources. You will also learn about the new ribbon interface of SharePoint Designer 2010 and you'll see how best to take advantage of this application by showing the new bells and whistles that come with this product.

MARCH 16, 2009 9AM - 4PM

PRECON WORKSHOP (IT PRO): SHAREPOINT JUMP START: REIMAGINING COLLABORATION

DAN HOLME

If you are new to SharePoint, or are trying to wrap your head around the massive potential of this powerful platform, you'll be the hero of your enterprise when you bring back the solutions you discover in this fast-paced, full-day pre-conference workshop. Dan Holme, a Microsoft MVP for SharePoint, will dive deep into the configuration, customization, and management of SharePoint collaboration. You'll learn to build SharePoint solutions that address common enterprise challenges, and you'll be amazed just how much you can do with Windows SharePoint Services (WSS) without having to pay for Microsoft Office SharePoint Server (MOSS). Topics include:

- SharePoint Administration Jump-Start: What you need to know to administer SharePoint effectively, in 90 minutes or less.
- How to use SharePoint document libraries as a replacement for traditional file shares.
- Driving effective collaboration and end-user adoption with Microsoft Office 2007 applications as SharePoint clients.
- How to build "Business Intelligence Lite", no-code, and low-code SharePoint solutions using Office 2007 and SharePoint Designer.

PRECON WORKSHOP (IT PRO): SHAREPOINT SERVER 2010: FARM UPGRADE AND WHAT'S NEW FOR EXPERIENCED SHAREPOINT ADMINS

SHANE YOUNG & TODD KLINDT

So you are already an awesome SharePoint v3 administrator and you want to start on the road to awesome for SharePoint 2010. Well then come on down. This workshop will start your road to SharePoint 2010 cool with a bang. In this workshop, we will cover everything you need to know to get your 2010 farm up and running. From there we will work through all of the new functionality that makes being an administrator so much furn. And if that wasn't enough fun, from there we will explore upgrade. We figure since you have a perfectly running farm now we might as well look at the upgrade story for your 2007 content. It'll knock your socks off.

PRECON WORKSHOP (DEVELOPER): BUILDING COMPOSITE APPLICATIONS USING SHAREPOINT DESIGNER 2010 AND THE BCS

RAYMOND MITCHELL

In this full-day workshop, you'll learn how to use the new functionality available in SharePoint Designer 2010 to build advanced Composite Applications. Some of the topics covered include:

- How to leverage the Data Form Web Part and the new XLV to display and interact with your SharePoint Data. We'll also take a long look at the magic behind these Web Parts–XSLT.
- How to use the updated Business Connectivity Services to surface your business data. We'll also explore other options to incorporate external data into your Composite Applications.
- How to create powerful Workflows and add Custom Actions to transform your Data Views and Dashboards into interactive Applications.
- How to customize the look and feel of your Composite Applications to create a rich user experience. We'll walk through several real-world scenarios and give you the tools you'll need to build your own applications on top of the SharePoint platform.

PRECON WORKSHOP (DEVELOPER): DEEP DIVE INTO SHAREPOINT 2010 WORKFLOWS

ROBERT L. BOGUE

The Office 2010 system includes a much better transition between user developed workflows and developer workflows. Learn how SharePoint Designer can be used to start your workflow development process, how InfoPath forms can be your forms solution for your workflows, and how Visio is a part of the workflow development process. Once we've developed a workflow with end-user tools, we'll take it into Visual Studio and enhance it with things that you can only do in Visual Studio. We'll end with a discussion of Site Workflows and how they can be used.

FEATURED SPEAKERS

TODD BAGINSKI
INTELLIGENT EFFECTS

ROBERT BOGUE
THOR PROJECTS

ANDREW CONNELL
CRITICAL PATH TRAINING, LLC

KIRK EVANS
MICROSOFT

STEVE FOX
MICROSOFT

SCOT HILLIER
SCOT HILLIER TECHNICAL SOLUTIONS, LLC

JOHN HOLLIDAY
JOHN HOLLIDAY & ASSOCIATES, INC.

DAN HOLME
INTELLIEM, INC.

TODD KLINDT,
SHAREPOINT911

MATTHEW MCDERMOTT
CATAPULT SYSTEMS

RAYMOND MITCHELL
INETIUM

MICHAEL NOEL
CONVERGENT COMPUTING

TED PATTISON
CRITICAL PATH TRAINING, LLC

ASIF REHMANI
SHAREPOINT ELEARNING.COM

THOMAS RIZZO
MICROSOFT

SHANE YOUNG
SHAREPOINT911

And many more... ***Check our Web site as we continue to update it with speaker pictures and bios!***

SharePointPro 2010 SUMMIT & EXPO

Hotel and Travel

Bellagio Resort & Casino, Las Vegas, NV

Grant yourself the luxury of discovery time as you explore the dramatic features which distinguish this exquisite Las Vegas resort from every other destination in the world. From dancing fountains to a breathtaking conservatory & botanical gardens to serenity-splashed pools & courtyards, plus a refreshing addition to your entertainment options, the world famous Fountains of Bellagio were destined to romance your senses. Take in a complimentary Las Vegas show of water, music and light thoughtfully interwoven to mesmerize its admirers.

HOTEL ACCOMMODATIONS BELLAGIO RESORT & CASINO

3600 Las Vegas Boulevard South, Las Vegas, NV 89119
Bellagio Resort & Casino is the conference site and host hotel.
This is where all sessions and activities are held.

We have secured a discount conference rate of $149 per night plus tax (12%). Based on Availability. Rate is based on single or double occupancy. Hotel requires a one night room and tax deposit at time of reservation. (Credit card will be charged by the hotel). Hotel cancellation policy: Must cancel at least 48 hours prior to arrival date.

Space is limited so reserve your room early by registering online or by calling the conference hotline at 800-438-6720 or 203-400-6121. All reservations must be guaranteed with a major credit card to confirm room. A deposit of the first night room and tax will be charged. Cancellations must be received by the hotel 48 hours prior to the confirmed arrival date to receive refund of deposit

AIRLINE

Please call Pericas Travel at 203-562-6668 for airline reservations.

CAR RENTAL

Hertz is offering auto rental discounts to attendees. See the conference Web site for details.

ATTIRE

The recommended dress for the conference is casual and comfortable. Please bring along a sweater or jacket, as the ballrooms can get cool with the hotel's air conditioning.

SPONSORSHIP/EXHIBIT INFORMATION

For sponsorship information, contact Jackie Baillie
949-226-2313 phone • E-mail Jacquelyn.baillie@penton.com
See Web site for more details. www.sharepointprosummit.com

TAX DEDUCTION

Your attendance to this conference may be tax deductible.
Visit www.irs.ustreas.gov. Look for topic 513 - Educational Expenses. You may be able to deduct the conference fee if you undertake to (1) maintain or improve skills required in your present job; (2) fulfill an employment condition mandated by your employer to keep your salary, status, or job.

GROUP DISCOUNT

Register individuals from one company at the same time and receive a group discount.

1-3 registrants	**$1,395 per person**
Additional registrants after the 3rd (4th, 5th, 6th...)	**$1,195 per person** ($200 off each)

Call 800-438-6720 to take advantage of group discount pricing.

Notes & Policies: The Conference Producers reserve the right to cancel the conference by refunding the registration fee. Producers can substitute speakers and topics and cancel sessions without notice or obligation. Updates will be posted on our Web site at www.sharepointprosummit.com. Tape recording, photography is not allowed at any session. Conference producers will be taking candid pictures of events and reserve the right to reproduce. By attending this conference you agree to this policy. You may transfer this registration to a colleague by notifying us before the start of the event. Please inform us if you have any special needs or dietary restrictions when you register.

Registration & Cancellation Policy: Payment must be received before the start of the conference. Cancellations by February 15th, 2010 must be received in writing and will be refunded minus a $100 processing fee. After February 15th, 2010 cancellations and no-shows are liable for full registration fee, however registration can be transferred to the next Connections Conference within 12 months or to another person.

CONFERENCE REGISTRATION • MARCH 16-19, 2010

FULL CONFERENCE REGISTRATION INCLUDES KEYNOTE ON MARCH 17TH,
THROUGH CLOSING SESSION MARCH 19TH, 4:30PM

NAME _____ PRIORITY CODE _____

COMPANY _____ TITLE _____

STREET ADDRESS (REQUIRED TO SHIP MATERIALS) _____

CITY, STATE, POSTAL CODE _____ COUNTRY _____

TELEPHONE _____ FAX _____ E-MAIL ADDRESS (IMPORTANT) _____

ONLINE: www.SharePointProSummit.com
E-MAIL: info@DevConnections.com
PHONE: (800) 438-6720
(203) 400-6121
FAX: (913) 514-9362
MAIL:
SharePointPro Summit & Expo 2010
c/o Tech Conferences, Inc.
731 Main Street, Suite C-3
Monroe, CT 06468

☐ **SharePointPro Summit & Expo** *before* JANUARY 15, 2010 ..... $1195 _____

after JANUARY 15, 2010 ..... $1395 _____

PRE-CONFERENCE WORKSHOPS TUESDAY, MARCH 16, 2010 LUNCH IS INCLUDED WITH FULL DAY WORKSHOPS ONLY.

☐ SharePoint Jump Start: Reimagining Collaboration HOLME ..... 9AM - 4PM ..... $399 _____

☐ SharePoint Server 2010: Farm Upgrade and What's New YOUNG & TODD KLINDT ..... 9AM - 4PM ..... $399 _____

☐ Building Composite Applications Using SharePoint Designer 2010 and the BCS MITCHELL ..... 9AM - 4PM ..... $399 _____

☐ Deep Dive into SharePoint 2010 Workflows BOGUE ..... 9AM - 4PM ..... $399 _____

CONFERENCE MATERIALS

FULL CONFERENCE REGISTRATION INCLUDES MATERIALS FOR THE CONFERENCE FOR WHICH YOU REGISTER;
YOU MAY PURCHASE MATERIALS FOR THE OTHER CONCURRENTLY RUN EVENTS.

☐ SharePointPro CD ..... $75 _____

☐ VirtualizationPro CD ..... $75 _____

TOTAL

☐ CHECK (payable to Tech Conferences) All payments must be in US Currency. Checks must be drawn on a US bank.
**IMPORTANT: Must reference which Connections conference you are registering for on your check.*

☐ CREDIT CARD ☐ VISA ☐ MASTERCARD ☐ AMEX

CREDIT CARD NO. _____ EXPIRATION DATE _____

Cardholder's Signature _____ Cardholder's Name (print) _____

Penton Media
c/o Tech Conferences, Inc.
731 Main Street, Suite C-3
Monroe, CT 06468

Mailroom: If addressee is no longer here,
please route to MIS Manager or Training Director

Using AD Recycle Bin For MAILBOX RECOVERY

Eliminate frustration by using logic—and this Server 2008 R2 tool

by J. Peter Bruzzese

When a user is accidentally deleted from Active Directory (AD), your first thought might be to panic. What happens to that user? How do I bring the user object back? What about the connection between the mailbox and the user? All excellent questions, and all best handled with logic. In logic, a conditional statement is a compound statement formed by combining two sentences (or facts) using "If/Then." For every *if* that might happen within your network, you need to know what your *then* will be.

For example, if a user is accidentally deleted from AD and if you're using Windows Server 2008 R2 with a forest level raised to Server 2008 R2 and the AD Recycle Bin enabled, then you will restore that user through Windows PowerShell by using the Restore-ADObject cmdlet. Wait: Perhaps we're moving a bit too fast with that last portion.

Let's take it from the top: Your options have broadened with the release of Server 2008 R2 and its new Active Directory Recycle Bin. Combining this new tool and the time-proven tool of logic, you can make troubleshooting deleted user objects and recovering users in AD easier.

The AD Recycle Bin lets you recover a deleted user object through the use of PowerShell or the LDP tool. In this article, I focus on Server 2008 R2 domain controllers (DCs) and Microsoft Exchange Server 2007 mailbox servers running on Server 2008/Windows Server 2003 member servers, although my discussion also applies to Exchange 2010 servers running on Server 2008 or Server 2008 R2 servers.

The only part of the process that has changed since Exchange 2000 is the recovery element. With Exchange 2000 and Exchange 2003 if you delete a user, the mailbox is deleted with it. That mailbox isn't permanently deleted but simply flagged for deletion and held for the duration of the mailbox retention period. After that period expires, the mailbox is purged. Although the mailbox is flagged for deletion, you can restore it using the Cleanup Agent on the Mailbox store. With the use of the AD Recycle Bin, you can recover your users quickly and reconnect them to their mailboxes within moments.

The AD Recycle Bin is a feature that must first be enabled for your organization. Before you can enable it, all your DCs within the forest need to be running Server 2008 R2, and you need to raise the forest functional level to Server 2008 R2 as well. (To learn more about the AD Recycle Bin in Server 2008 R2, plus how to enable it and undelete an object from it, see www.windowsitpro.com, InstantDoc IDs 102221, 102222, and 102224.) To enable the AD Recycle Bin, open PowerShell and use the Enable-ADOptionalFeature cmdlet and the necessary syntax to enable it specifically for your environment. The three FAQs I mentioned and Microsoft's "Step 1: Enable Active Directory Recycle Bin" at technet.microsoft.com/en-us/library/dd379481%28WS.10%29.aspx tell more about

how to enable the Recycle Bin. After you enable the Recycle Bin feature for AD, all items that are deleted will be restorable because the Recycle Bin will look for the IsDeleted attribute set to True; an object with that setting can be brought back from that point.

Troubleshooting

Keep in mind that there are two different sides to this story: the AD side and the Exchange side. In many small to midsized organizations, these two sides are combined and one person oversees them (or a small team of people who have permissions and access within both). In larger companies, however, you might be dealing with two separate teams. In that case you will need cooperation between the two to accomplish the goal of recovering a user and reconnecting that user to the mailbox.

To understand the process of troubleshooting a deleted user or deleted mailbox, keep a few facts in mind. A functioning user mailbox requires three things:

- A user object must exist (or be created during the mailbox creation process) in order to attach or assign the Exchange mailbox attributes to it.
- Exchange attributes are tied to a user object.
- The user must either log on or receive mail to that mailbox. When you create a mailbox, Exchange attributes are added to the user object in AD; however, the associated mailbox data isn't added until you log on or receive mail.

To restore a user by using the Get-ADObject cmdlets, you need to be running Server 2008 R2 (or Windows 7 as part of Remote Server Administration Tools—RSAT), because the AD module for PowerShell is part of the new features in Server 2008 R2 and the module can only be installed on Server 2008 R2 or Windows 7 systems. The RSAT tools let you manage roles and features that are installed on computers that are running Server 2008, Windows 2003, and Server 2008 R2. (They can be downloaded at www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=7d2f6ad7-656b-4313-a005-4e344e43997d.)

Now, let's use those If/Then statements I mentioned at the beginning of this article. Every If statement implies a Then as you troubleshoot the problem.

What happens if a user is deleted from AD using the AD Console or Active Directory Users and Computers? Does his mailbox remain in the recipients container? Does it move over to the Disconnected Mailbox section? Is it lost forever?

If you delete a user, the mailbox also disappears. To restore both, you would use the AD Recycle Bin cmdlets in PowerShell; restoring the user automatically restores the mailbox as well. So, for example, if the user is "Logan Smith," and that user has been deleted from the Active Directory Users and Computers console, you would open a PowerShell prompt on the DC (for the sake of ease) and type:

```
Get-ADObject -Filter
  {displayName -eq "Logan Smith"}
  -IncludeDeletedObjects |
  Restore -ADObject
```

The result: The user object is restored and the mailbox is restored to the Recipients container in Exchange as well. Two items get corrected in one step. Note that I'm only talking about the server side of Server 2008 and Server 2008 R2 for the restore in this way. You could have legacy servers in play but for the most part I am looking at Exchange 2007 and Exchange 2010.

What happens if you right-click a mailbox in the Recipients container and choose Disable? The mailbox goes to the Disconnected Mailbox section. (This doesn't mean items are removed from the mailbox database; instead, it just puts the mailbox in a safe, limbo state.) You can, at that time, restore the mailbox to its original user or you can choose to restore the mailbox to another user. Note that one of the benefits of this approach is that you can restore a mailbox of a former employee to another user.

What happens if you disable a mailbox, then delete the user account that was associated with that mailbox? The mailbox is still available for the length of time set for the Deleted Mailbox Retention period. You can create a new user and connect the mailbox to that new user (or to an existing user who doesn't have an associated mailbox) or you can use the AD Recycle Bin to restore the user who was deleted. But the trick is to reconnect the mailbox to the user who was deleted if that was your intent. It won't happen automatically like it does if you delete a user account and the mailbox is still connected to the user at the time.

The result: You've completed a two-step process. You restored the user object, then reconnected the mailbox to that user.

What if you right-click a mailbox and choose Remove from the menu options? The warning says the user object will be removed and the mailbox will be marked

A Free GUI–Based AD Recycle Bin Tool

The AD Recycle Bin tool in Windows Server 2008 R2 is a long time coming, yet frustrating on many fronts. For one thing, it isn't installed by default. For another, it requires use of the command line. Finally, it's available only in Server 2008 R2.

A free alternative is Overall Solutions' ADRecycleBin tool. This GUI–based solution works with the Server 2008 R2 Recycle Bin by restoring objects, or it can reanimate objects if you're using an earlier form of Active Directory or simply can't bring up your forest functional level. Essentially, it looks for tombstones and presents them to you for a simple click-restore of those items. You don't have to install it prior to the deletion because it will simply look for the IsDeleted attribute on objects to gather a graphical view of tombstones. You can find the tool at the Overall Solutions website: www.overall.ca/index.php?option=com_content&view=article&id=40:adrecyclebin&catid=15:adrecyclebinexe&Itemid=64.

for removal as well. Here is where we see all the information we have collide. The user will be removed from AD. The mailbox will be placed in the Disconnected Mailboxes section. However, this time, restoring the user doesn't automatically restore the mailbox as it did when we deleted the user account form with the AD console. Restoring the user account from the Recycle Bin will restore the account only. You will still have to reconnect the mailbox with that account, if that is your goal.

A Review of Options

Keep in mind that this entire exercise was meant to supply all the facts that you need to form logical resolutions to problems that occur when items are deleted. You just put the facts into simple statements of If/Then.

- If an AD user has a functioning mailbox (that is, the user logged on to it or received mail in it) and if that user is deleted from within the AD tools, then the mailbox disappears with the user. Both will be restored when you use the AD Recycle Bin.
- If that same user's mailbox was disabled before being deleted, then the mailbox would have moved over to the Disconnected Mailbox location. It could be reattached to that user when it's restored using the Recycle Bin, or it could be attached to another existing or newly created user object that currently has no mailbox attached.
- If the mailbox is removed from within the Exchange Management Console, the user object would be removed at that time and the mailbox would be moved over to the Disconnected Mailbox items. Upon restoration of the account, the mailbox would have to be reconnected manually.

You can see that the entire procedure is somewhat like a choreographed dance. In the event you have a small environment and you are the only administrator handling all the parts, you can consider all of these facts and map out a plan of attack depending on the circumstances. If, however, you are in a much larger environment with both an AD and an Exchange team, you can see how you would first need to determine the timeline of moving to Server 2008 R2, ensure the AD team understands the importance of turning on the Recycle Bin, and make sure the AD team knows how to restore users through PowerShell. (If you accidentally delete a user object and think you will simply turn on the Recycle Bin at that time and restore the object, you'll be disappointed. When you enable the AD Recycle Bin, all objects that have been deleted already are recoverable only through an authoritative restore from a backup of AD that was taken prior to the implementation of the AD Recycle Bin.)

> Your options broadened with the release of Server 2008 R2 and its new Active Directory Recycle Bin. Combining this new tool and the time-proven tool of logic, you can make troubleshooting deleted user objects and recovering users in AD easier.

At the same time, the teams need to communicate to ensure a user isn't deleted from AD prior to the Exchange team disconnecting the mailbox from that user (if it's an environment where the mailbox is reattached to another user or held as Disconnected for a period of time). In addition, the Exchange team should know how and when to restore disconnected mailboxes to restored, newly created, or preexisting user accounts.

When Too Much Time Has Passed

As time passes, the clock is ticking on objects in AD. They will eventually be permanently deleted if they aren't recovered before their lifetime is up. The default IsDeleted lifetime is actually the same as the tombstone lifetime (which is what the object becomes if you don't have the Recycle Bin enabled)—by default, 180 days. At this point the object moves toward the 'garbage collection' phase and can't be recovered without a backup and restore solution. AD object restore on that level is another article entirely.

The same is true of mailbox retention times. After those times have been exceeded, the mailbox is unrecoverable without a backup solution. Many different solutions exist through third-party vendors. One of the negative issues with Server 2008 is the loss of an onboard backup solution for Exchange. There is an "almost-fix" in Exchange 2007 SP2, but it lets you back up only the volume itself. So, if you want a more precise and granular backup for mailboxes, you need to consider options beyond what Server 2008 or Exchange offers. You might consider System Center Data Protection Manager and perhaps restore a database over to a recovery storage group or database. Then you can recover the lost mailbox. Or you might try another solution that allows for immediate recovery of the mailbox, such as Mimosa NearPoint for Exchange or CommVault Simpana. The sidebar "A Free GUI–Based AD Recycle Bin Tool" on page XX discusses a free tool that can also help. Whatever choice you make as to recovery software, it doesn't hurt to try to solve these If/Then scenarios yourself first.

Logic Beats a Restore from Backup

By using logic, plus the AD Recycle Bin and the Disconnected Mailbox location, you can avoid the frustration of restoring from a backup. These tools can save admins a lot of frustration, stress, and panic.

InstantDoc ID 103272

J. Peter Bruzzese
(jpb@cliptraining.com) is a triple-MCSE, MCT, and MCITP: Messaging, as well as a *Windows IT Pro* contributor and author of *Windows Server 2008 How-To* (Sams). He is cofounder of ClipTraining.com.

FEATURE

How to Efficiently Search and Manage Event Log Data

Event Viewer and other log tools in Windows Server 2008 can save you time

by Orin Thomas

It's no secret that checking event logs is tedious. I'd like to show you some techniques you can use and new technologies available in the Windows Server 2008 Event Viewer that let you zero in on specific events of interest. Rather than having to check the contents of each different log, you can configure Windows to alert you when something interesting has happened. Plus you can efficiently search and present event log data so you can get on with the rest of the tasks that take up your day.

Knowing What to Look For

Searching through event logs for evidence of a particular event can be like looking for a needle in an event log haystack, especially if it's not immediately obvious whether you should be checking fields such as String, Messages, Data, EventType, EventTypeName, EventCategory, or EventCategoryName. You might suspect that an event has occurred and has even been logged, but you might not be sure what evidence exists of that event within the event log.

The key to effectively examining event logs is knowing what to look for. Rather than searching all event log fields using key terms, searching for specific events by their event ID is a more effective way of locating evidence. The catch is that you have to know what event ID correlates to a specific event. The event IDs in a Server 2008 event log are all well documented, either on TechNet or elsewhere. I'll cover a few event IDs of interest a little later in this article.

IT pros should note that Server 2008 event IDs use a different numbering system to those used in earlier versions of Windows. For example, an account lockout is recorded as event ID 644 in Windows 2000 Server and Windows Server 2003 event logs, but event ID 4740 records account lockouts on Server 2008. This new numbering system means that existing scripts that trawl logs for event IDs related to events in Windows 2003, Windows XP, and Win2K won't work when you run them against the logs on a computer running Server 2008.

Some notable Server 2008 security event IDs are listed in Table 1. These events are primarily security related. Some of them might be entirely benign, but if any of them occur with great frequency in your environment, it might be worth investigating further. You can find a list of all Server 2008 security-related event IDs at support.microsoft.com/kb/947226.

Filtering and Custom Views

Filters are quick-use tools that let you limit the displayed data in a single log. Filters in Server 2008 work mostly the same way as they did in Windows 2003. Although filters aren't persistent, you can save a filter as a custom view. To create a filter on a Server 2008 computer, perform the following steps:

1. Open Event Viewer.
2. Click the log that you want to filter, then click Filter Current Log from the Action pane or right-click menu. This will open the Filter Current Log dialog box, which Figure 1 shows.

Table 1: Notable Windows Server 2008 Security Event IDs	
Event ID	Message
4777	The DC failed to validate the credentials for an account
4771	Kerberos pre-authentication failed
4772	A Kerberos authentication ticket request failed
4723	An attempt was made to change an account's password
4724	An attempt was made to reset an account's password
4738	A user account was changed
4740	A user account was locked out
4767	A user account was unlocked
4780	ACL was set on accounts which are members of administrators groups
4625	An account failed to log on locally
4649	A replay attack was detected
5378	The requested credentials delegation was disallowed by policy
4621	Administrator recovered system from CrashOnAuditFail, Users who are not administrators will now be allowed to log on

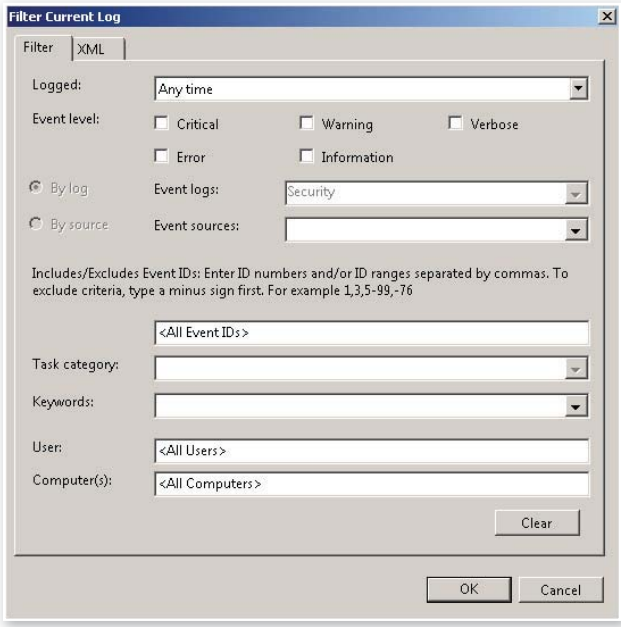


Figure 1: Filter Current Log dialog box

3. You can specify a time period if you know approximately when events occurred. You can specify the event level, choosing between Critical, Warning, Verbose, Error, and Information. If you select none of these, all event levels will be returned. You can't modify which event log is being checked because filters apply only to a single log.

4. You can choose the event sources that generated the log entries, and search for keywords, users, or computers. You can also enter specific event IDs.

As I mentioned earlier, the easiest way to look for specific events is to enter event IDs. The drawback to filtering on the basis of event ID is that you need to know the ID of the event that you are looking for. Searching by user or computer doesn't return all events relating to that user or computer.

For example, if an account logon event is associated with the user displayed as N/A, it is only by looking within the EventData field that you'll actually see the user name that was logged on. You can't enter freeform keywords, but can only select from a list of event-related keywords.

A custom view is essentially a filter that you can reuse and apply to multiple event logs. Custom views are new to Server 2008. As you can see in Figure 2, page 46, where a custom view has been created to show all events related to ID 4738, custom views get their own node within the Server 2008 Event Viewer. To create a custom view, perform the following steps:

1. Open Event Viewer from the Administrative Tools menu.

2. Right-click the Custom Views node, then click Create Custom View.

3. Unlike with a filter, you can configure a custom view to extract data from multiple event logs. As you can see in Figure 3, page 46, the options that you can configure are similar to what is available when configuring a filter.

Another useful feature of custom views is that you can export them, then import them on other Server 2008 computers. This lets you better manage the time you spend going through logs. Rather than scanning the logs for specific events, you can configure a custom view to present all interesting events that have occurred on a computer in a single location. This is because unlike filters, custom views can apply to multiple logs. Once you have set up an effective custom view, you can then place that custom view on each computer where you need to regularly review the event logs. Rather than having to trawl through every log on the server, you only have to look at a single list, because the custom view will contain all events that you have defined as interesting. Custom views can function as a single port-of call, ensuring that you don't miss an important event.

Scanning Logs from the Command Line

Although custom views and filters can provide you with a list of interesting events, you can't use these tools to summarize the information contained within event logs. You can use a custom view to see all of the failed logon events, but you need to use other tools to summarize failed logon events on the basis of user account. Perhaps the most famous Windows log tool is Log Parser, which can be downloaded for free at www.microsoft.com/downloads/details.aspx?FamilyID=890cd06b-abf8-4c25-91b2-f8d975cf8c07.

Log Parser lets you query event logs using SQL syntax. For example, the following Log Parser command provides you with a list of accounts that have been added to the Administrators, Domain Admins, or Enterprise Admins groups:

```
logparser –i:evt "select extract_token
  (Strings,0,'|') from Security where
  EventID IN (4780)"
```

Although Log Parser works well with Server 2008, it hasn't been updated since January 2005. This suggests that support for the tool

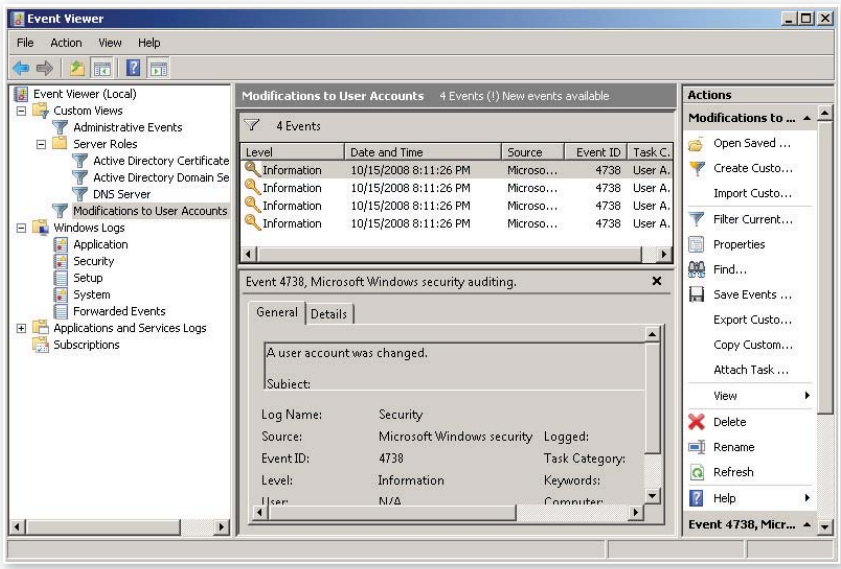


Figure 2: Custom views interface

may be deprecated in favor of Windows PowerShell. It's possible to write scripts in PowerShell that accomplish exactly the same things that you can accomplish using Log Parser.

Unfortunately, as amazing as PowerShell is, unless you are comfortable with it, you won't find its syntax as intuitive as Log Parser. The following PowerShell command, executed from an elevated PowerShell prompt, also retrieves data related to event ID 4780:

```
Get-Eventlog -logname Security | where
 {$_.EventID -eq "4780"} | Format-Table
 -Wrap TimeWritten,Message
```

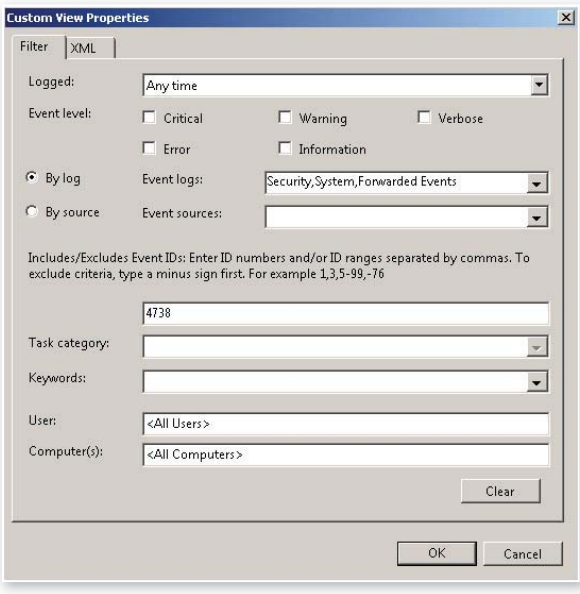


Figure 3: Creating a custom view

Finally, you can also use the wevtutil.exe command-line utility to examine event logs. Wevtutil.exe can be very useful on Server 2008 Server Core computers that don't support PowerShell. The following command locates events with event ID 4780 in the security log:

```
Wevtutil qe Security /rd:true /f:text /q:
  *[Security[(EventID=4780)]]
```

The biggest drawback to the wevtutil.exe utility is the lack of documentation on how to use it. It also can't be configured to collate data, unlike PowerShell and Log Parser, which can. I include Wevtutil here only for the sake of completeness.

Event Forwarding

Event forwarding is a new Server 2008 feature that allows events to be forwarded from one Server 2008 computer to another over the HTTP protocol. The advantage of this is that you can set up the equivalent of a log collection server, so rather than having to check the event logs of each computer on the network for specific events, you can check for events from many computers in a single place.

Consider account logon events. Any domain controller (DC) in your organization can authenticate a particular user's logon. To determine which DC authenticated a logon, you check the security logs of each DC in your domain, though the DC that authenticates a logon is almost always located at the same site as the client logging on.

With event forwarding, you can forward all events, or just specific events, which you can define using a collection filter, to a central computer called a collector. Rather than having to check each DC in the domain, you just check the collector computer that has copies of the account logon events from all DCs in the domain. Server 2008 lets you configure two types of event log subscriptions:

Collector-initiated subscription. With this subscription type, a central computer polls a set of source computers to retrieve event log data. Collector-initiated subscriptions require manual configuration on each source computer as well as the collector computer. This involves running *winrm quickconfig* from an elevated command prompt at each source computer, which allows remote management and configures a firewall exception. You also need to add the computer account of the collector computer to the local Administrators group on each source computer. I cover configuring a collector computer later in this section.

Source-initiated subscription. When you configure a source-initiated subscription, each computer forwards events to a collector computer. You can configure source-initiated subscriptions using Group Policy. You do this by editing the *Configure the Server Address, Refresh Interval, and Issuer Certificate* policy located under the \Computer Configuration\Policies\Administrative Templates\Windows Components\Event Forwarding node.

Configuring the collector computer is similar for both the collector-initiated subscription and source-initiated subscription methods. To do this, perform the following steps:

1. Open an elevated command prompt and type

```
winrm qc -q
```

and then

```
wecutil qc /q
```

This configures Windows Remote Management and the Event Collector service.

2. Open Event Viewer, right-click the Subscriptions node, and click Create Subscription to open the Subscription Properties dialog box, shown in Figure 4.

3. Choose between a collector-initiated and source-initiated subscription. If you choose collector initiated, you must select individual computer accounts. If you choose source initiated, you must select computer groups that you have configured using Group Policy.

4. Use the Select Events button and perform a process identical to creating a custom view to select the types of events the collector computer gathers or forwards. The default settings are for the collector computer to place forwarded events into the Forwarded Events log, though you can configure a different destination instead. You can apply custom views, filters, or scan the Forwarded Events log using Log Parser or the Get-EventLog function of PowerShell.

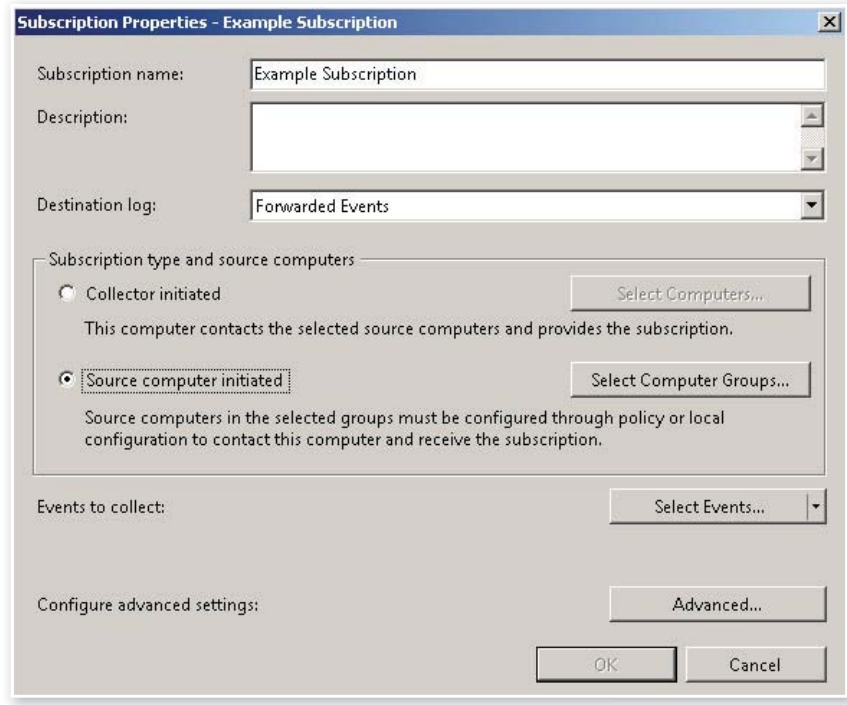


Figure 4: Subscription properties

Being Alert

Event Viewer tasks let you start a program or send a message or an email whenever a particular event occurs, and that event is logged to the Server 2008 event logs, including an event written to the Forwarded Events log on a collector computer. Configuring such a task ensures that you are made aware of the event at the time it occurs, not when you get a chance to review the event logs later. Event Viewer tasks are similar to the alert triggers that are available in Windows 2003 but simpler to configure, because in Windows 2003 you have to configure triggers from the command line using the eventtriggers utility.

In Server 2008 you can create an event trigger directly from Event Viewer by right-clicking an event and selecting Attach Task To This Event. This launches the *Create a Basic Task* wizard, in which you specify what action you want Windows to take when a new event that has this event ID is logged. You can also create an Event Viewer task using the Task Scheduler console:

1. Open the Task Scheduler from the Administrative Tools menu. Expand the Task Scheduler Library node.

2. Right-click the Event Viewer Tasks node, then click Create Task. The Event Viewer Tasks node is created when you create a task triggered by an event in Event Viewer. This launches the Create Task dialog box. Enter a name for the task. Also ensure that you enable the *Run whether user is logged on or not* option; otherwise the Event Viewer task will not be triggered after you log off.

3. On the Triggers tab, click New to configure a new trigger. On the *Begin the task* drop-down menu, select *On an event.* Then select the event ID and the log that you want to trigger the task.

4. On the Actions tab, select what type of action should occur when the specified event is detected. You can configure the Event Viewer task to run a script or program, send an email, or send a message. You should only use the message option if you want a logged-on user to be notified directly.

Event Viewer tasks can be imported and exported, so you can deploy them easily on multiple servers throughout your organization. You remove Event Viewer tasks through the Task Scheduler console and not through Event Viewer.

You should be careful in selecting which Event Viewer tasks you set up. If you configure too many Event Viewer tasks to alert you, you will be deluged with notifications and will most likely begin to ignore them. You should choose events such as event ID 4780 (see Table 1), which should happen rarely but are important enough to demand your attention.

Limit Data to Data of Interest

The key to dealing with event logs is being able to zero in directly on the data that is of interest to you. I discussed how you can view only interesting events using filters and custom views, how you can search logs using Log Parser and PowerShell, how you can centrally collect logs using event log forwarding, and how you can be notified as soon as an interesting event occurs by using Event Viewer tasks. In combination, all of these techniques can reduce the area of haystack that you have to deal with, making it a lot simpler to locate relevant needles.

InstantDoc ID 103240

Orin Thomas
(orin@windowsitpro.com) is a contributing editor for *Windows IT Pro* and a Windows Security MVP. He has authored or coauthored more than a dozen books for Microsoft Press.

FEATURE

Document Your Domain Groups

This admin script lets you generate invaluable reports about your group structures

by Jim Turner

I recently wrote an admin script that produces a very thorough single-domain listing of all your Active Directory (AD) groups in a nicely formatted, easy-to-read layout. The report the script produces provides you with an excellent point-in-time group history document and supplies a great deal of information to you, your security department, and your auditors. This isn't your typical group-listing script; it provides invaluable reports as well as a permanent record of your group structures. Here's a list of the script's major features:

- Enumerates all domain groups within a single domain
- Lists and enumerates all nested groups
- Presents information in one Excel document with each group on its own worksheet
- Lists users whose primary group is the group being enumerated (these members don't normally show up in group listings unless you take care to account for this situation as this script does; for example, if you set your primary group to Domain Admins and do a simple group listing of that group, you won't see yourself as a member in that listing)
- Colors nested group names in red and recurring groups in purple
- Avoids possible endless loops should one group contain another group that contains the first group
- Sorts and indents by group
- Provides a domain group summary list with hyperlinks to all groups that have members
- Provides a no members summary list if there are any groups without members, including hyperlinks to the groups
- Colors worksheet tabs in red for easy identification of groups with no members
- Uses blue text for disabled user accounts within groups
- Provides total group counts for both groups with and without members

Script Overview

The script cycles through a collection of groups within a single AD domain and writes each group's members and nested group members into its own specific Excel worksheet. (You can download the script by going to www.windowsitpro.com, entering 103358 in the InstantDoc ID box, clicking Go, then clicking the *Download the Code Here* button.) In the end, all the individual domain group worksheets make up the overall domain group listing spreadsheet. In addition to the individual group worksheets, a summary worksheet is created and, if any groups have no members, an additional worksheet is created listing all the groups that have no members.

During the process of evaluating individual groups, disabled accounts are highlighted in blue. Any nested groups are indented and highlighted in red and members of those nested groups are also

indented and listed under their specific parent group.

If a specific nested group happens to occur more than once in any specific listing, it's not enumerated again but rather highlighted in purple; you'll find that the fully enumerated group already exists elsewhere within that group listing. A summary worksheet is created at the end of the process, providing group total information and easy-to-use hyperlinks to all your groups for quick and easy analysis.

If a specific nested group happens to occur more than once in any specific listing, it's not enumerated again but rather highlighted in purple; you'll find that the fully enumerated group already exists elsewhere within that group listing.

If your domain has any groups that do not contain members, a separate groups with no members worksheet is created, providing the names and hyperlinks to those groups that have no members.

The resulting spreadsheet with its color coding and nested group indentation scheme provides a very thorough and easy-to-comprehend picture of your domain's group infrastructure.

How It Works

Aside from setting up some variables, constants, and an instance of Excel, the first process the script undertakes is to create a dictionary that contains a list of all disabled accounts. This is done by querying AD. The dictionary is used at a couple of key points within the script while enumerating group member users to determine if the user account is disabled or not. You'll see this later on in the script. If an account is disabled, that user ID is formatted in the Excel output with a blue font, making it easy to spot within the group listings.

Next, a collection of all domain groups is gathered using the simple AD query shown in Listing 1. Stepping though the group collection constitutes the main loop of the script, where all groups are ultimately enumerated. Within this main loop a call is made to the GetGroupMembers subroutine, which is really the workhorse of this whole process. It's within the GetGroupMembers subroutine that each group's membership is individually evaluated and written to the Excel report.

Inside the Subroutine

Once a specific group object is passed to the GetGroupMembers subroutine, the process of enumerating the members of that group begins. The code shown in Listing 2 performs an often-overlooked process: checking for user accounts that have a primary group assignment that belongs to the group being evaluated. As strange as it may sound, user accounts whose primary group is the group being evaluated will not be part of the collection returned with an AD group query. To account for this condition, you must approach it from another angle, which is to look for accounts whose PrimaryGroupToken is that of the group you're evaluating.

The chunk of code in Listing 2 ensures that you capture these members. You'll see that I also trigger a flag within this section of code to indicate that this group "Has Members" whenever a user or group exists within the group being evaluated. By triggering, I mean I change the value of the HasMember variable from False to True. If this flag isn't triggered while evaluating the group, I can capture the group name to a dictionary called NoMembersList, which is used near the end of the program to list all the groups with no members. If the flag is triggered (set to True), the group is stored to a dictionary called YesMembersList, which is used to list all the groups that do have members. You'll also notice that within this section of code I check to see if the user item is found within the DisabledAccounts dictionary and highlight the output in blue if the user ID exists within the dictionary.

After checking for the primary group, the script starts to enumerate the group's members, as seen in the section of code in Listing 3. The process here is mainly

Listing 1: AD Query that Collects the Domain Groups

```
LDAPFilter = "(&(objectCategory=person)(objectClass=user)
     (userAccountControl:1.2.840.113556.1.4.803:=2))"
strQuery = "<LDAP://" & DNC & ">;" & LDAPFilter &
     ";samaccountname;subtree"
objComm.CommandText = strQuery
Set objRec = objComm.Execute
objRec.MoveFirst
```

Listing 2: Checking for User Accounts that Have a Primary Group Assignment

```
'*** Some admins tend to make their primary group Domain Admins
'*** Those will not show up when querying group membership
'*** Need to look for users that have this groups PrimaryGroupToken
Grp.GetInfoEx Array("primaryGroupToken"),0
tokName = Grp.Get("primaryGroupToken")
LDAPFilter = "(primaryGroupID=" & tokName & ")"
strQuery = "<LDAP://" & DNC & ">;" & LDAPFilter & ";adspath,samaccountname,cn;subtree"
objCommand.CommandText = strQuery
Set objRecordset2 = objCommand.Execute
Do Until objRecordset2.EOF
  HasMembers = True
  XL.Cells(Row,col).Value = objRecordset2.Fields("samaccountname").Value &
     " (" & objRecordset2.Fields("cn").Value & ")"
  XL.Cells(Row,256).Value = sortgroup & " " & objRecordset2.Fields("cn").Value

  USam = ""
  USam = objRecordset2.Fields("samaccountname").Value
  If DisabledAcct.Exists(USam) Then
   XL.Rows(Row & ":" & Row).Font.Color = RGB(0,0,255)
   XL.Cells(Row,col).Value = XL.Cells(Row,col).Value + "(Disabled Account)"
  End If

  Row = Row + 1
  objRecordset2.MoveNext
Loop
objRecordset2.Close
```

concerned with whether the member is a regular account or whether it's a group member. If it's a regular account, the member goes through the same process it did when checking the primary group members: The group member is checked against the disabled accounts dictionary and colored if it is a disabled account and the HasMembers flag is set to True.

If the member is another group, the group is evaluated against the group dictionary. If the group doesn't exist, it's added to the group dictionary and a recursive call is made to the GetGroupMembers subroutine to gather the members of that particular nested group.

If the nested group exists in the group dictionary, the recursion process is not undertaken; the group name is simply written to the worksheet, colored purple, and the script moves on to the next group member. Keeping track of groups in the group dictionary in this fashion prevents the possibility of the code going into an endless loop if a group happens to contain another group that contains it as a member.

Keeping track of groups prevents the code from going into an endless loop if a group contains another group that contains it as a member.

Listing 3: Enumerating Group Members

```
For Each memobj In Grp.Members
 If Lcase(memobj.Class) = "group" Then
  HasMembers = True
  '*** Add to dictionary if it does not already exist
  If Not dictObj.Exists(memobj.samaccountname) Then
   dictObj.Add memobj.samaccountname,memobj.samaccountname
   XL.Rows(Row & ":" & Row).Font.Color = RGB(255,0,0) 'make groupname red
   XL.Cells(Row,Col).Value =  memobj.samaccountname  & " (" & memobj.cn & ")"
   '*** Since group changed, concat groupname to sortgroup
   '*** Asterisk is used as a separator
   sortgroup = sortgroup + "*" + memobj.name
   XL.Cells(Row,256).Value =  sortgroup
   Row = Row + 1
   '*** Increase indent for new group
   Col = Col + 1
   '*** Store new groupname to savegroup
   savegroup = memobj.name
   '*** Recurse subgroups
   GetGroupMembers(memobj)
  Else
   '*** This group has already been enumerated. Make reoccurring groupname purple
   XL.Rows(Row & ":" & Row).Font.Color = RGB(255,0,255)
   XL.Cells(Row,col).Value =  memobj.samaccountname & " (Reoccurring Group)"
   '*** Since group changed concat groupname to sortgroup
   '*** Asterisk is used as a separator
   sortgroup = sortgroup + "*" + memobj.name
   XL.Cells(Row,256).Value =  sortgroup
   Row = Row + 1
   '*** Since not enumerating group - remove reoccurring groupname from sortgroup
   sortgroup = Left(sortgroup,instrrev(sortgroup,"*")-1)
  End If
 Else
  HasMembers = True
  '*** ... Not a group
  XL.Cells(Row,col).Value =  memobj.samaccountname  & " (" & memobj.cn & ")"
  XL.Cells(Row,256).Value =  sortgroup & " " &  memobj.cn

  USam = ""
  USam = memobj.samaccountname
  If DisabledAcct.Exists(USam) Then
   XL.Rows(Row & ":" & Row).Font.Color = RGB(0,0,255)
   XL.Cells(Row,col).Value = XL.Cells(Row,col).Value + " (Disabled Account)"
  End If

  Row = Row + 1
 End If
 '*** Remove indent if group is no longer the same
 If savegroup <> grp.name Then
  Col = Col - 1
 '*** Store current groupname to savegroup
  savegroup = grp.name
 '*** Remove last group from sortgroup string
  sortgroup = Left(sortgroup,instrrev(sortgroup,"*")-1)
 End If
Next
```

Without going into a complicated explanation involving the indenting process, let me summarize what I do within the code to make sure the indentation stays accurate and the group members and nested groups are indented and sorted properly. Typically, formatting wouldn't be a problem for groups that just had users as members; you could easily sort on column A. But it's a different story when nested groups are involved. If a nested group is encountered when enumerating a group, I write the nested group under its parent group and then increase the column number by one so that the nested group's members appear indented by one column to the right. I also keep track of the group names whenever I enter a recursive call that sends the script off to enumerate a nested group. So when the recursive call is finished and the current group name is no longer the same as the one stored, I decrease the indent by subtracting one from the current column number, thus putting me back into the correct column of the previous group.

Even though the indentations might seem to be sufficient for having all the group information sorted properly, it is not sufficient for groups that contain other groups. Under normal circumstances, when a group with users and nested groups is enumerated you'll see that your first item in the collection might be a user, the second might be a group, the third might be another user, and so on. Therefore your users would not necessarily all fall under each other but would rather be separated by groups in between them. Technically, the listing would still be correct; however, visually this could make analyzing the data a bit confusing.

The piece to this process that helps keep things sorted properly involves writing the current overall nested group hierarchy level of each group member to the 256th column (which has column heading IV). To help understand this, a picture is truly worth a thousand words. So let's take a look at Figure 1 and Figure 2. Here you'll see an example of a fairly complex nested group listing.

	A	B	C	D	E	F
1	RTC Local User Administrators					
2	MarkH (Mark Hassall)					
3	RTCDomainUserAdmins (RTCDomainUserAdmins)					
4		MichaelH (Michael Holm)				
5	VPNUsers (VPN Users)					
6		CraigP (Craig Playstead)				
7		Domain Admins (Domain Admins)				
8			Administrator (Administrator)			
9			MeganS (Megan Sherman) (Disabled Account)			
10			MikeF (Mike Fitzmaurice)			
11		RTCDomainUserAdmins (Reoccurring Group)				

RTC Server Applications | RTC Local User Administrators | RTC

Figure 1: Nested group hierarchy

	IV
1	RTC Local User Administrators
2	CN=RTC Local User Administrators Mark Hassall
3	CN=RTC Local User Administrators*CN=RTCDomainUserAdmins
4	CN=RTC Local User Administrators*CN=RTCDomainUserAdmins Michael Holm
5	CN=RTC Local User Administrators*CN=VPN Users
6	CN=RTC Local User Administrators*CN=VPN Users Craig Playstead
7	CN=RTC Local User Administrators*CN=VPN Users*CN=Domain Admins
8	CN=RTC Local User Administrators*CN=VPN Users*CN=Domain Admins Administrator
9	CN=RTC Local User Administrators*CN=VPN Users*CN=Domain Admins Megan Sherman
10	CN=RTC Local User Administrators*CN=VPN Users*CN=Domain Admins Mike Fitzmaurice
11	CN=RTC Local User Administrators*CN=VPN Users*CN=RTCDomainUserAdmins

RTC Server Applications | RTC Local User Administrators | RTC Local

Figure 2: Sorting the group hierarchy by complete path

In Figure 1 you'll see that the group being processed is named RTC Local User Administrators. It contains one user—Mark Hassall—and two nested groups—RTCDomainUserAdmins and VPNUsers (note the red font, indicating they are groups). These three members fall directly under RTC Local User Administrators in column A. You'll see that the RTCDomainUserAdmins group has only one member—Michael Holm—and that it is indented to indicate that it belongs to the RTCDomainUserAdmins group. The VPNUsers group contains one user—Craig Playstead—and two nested groups—Domain Admins and RTCDomainUserAdmins—and they are indented one level to indicate that they belong to the VPNUsers group. The Domain Admins group members are indented as well to show they belong to the Domain Admins group. And finally, you'll see that the VPNUsers member RTCDomainUserAdmins is colored with a purple font and also has a notation indicating it is a recurring group and, therefore, you will not see indented members listed under it. You can, however, find the RTCDomainUserAdmins group in the listing and ascertain who the members of that group are.

Sorting It Out

To ensure that all my group listings would be sorted properly, I needed a single column to sort on that was structured in a fashion that would guarantee everything fell into its proper place. As you can see in Figure 2, by simply keeping track of the complete path of each group member's hierarchical structure and writing that to column 256 I could sort the worksheet on column IV and everything would fall right into place. The asterisks are used as a delimiter to mark the change in the hierarchy.

Wrapping It Up

The process of evaluating my groups continues until every group in the domain is evaluated. The process then exits the main loop and the script begins to wrap things up by providing group summary information and hyperlink listings to all groups with and without members. Accessing any particular group is simply a matter of clicking on the group name hyperlink. Note that if all your groups do contain members there will not be any references to "No Members."

I think that you'll find that having this documented within Excel has its advantages. Everything is contained within one file and all the groups are contained within their own individual worksheet. And if you need to know which groups a specific user belongs to you can easily use the "Find All" feature in Excel and locate every occurrence of that user. You could also use the "Find All" feature to locate everywhere a disabled account appears or where you had recurring nested groups, which could ultimately help you find inconsistencies that might exist within some of your group structures.

This script is a very useful admin utility that will provide invaluable reports as well as a permanent record of your group structures for any given point in time. It will also save you a lot of time and serve you and your auditors well if you are asked to provide detailed group information during the hectic audit season.

InstantDoc ID 103358

Jim Turner
(jturnervbs@gmail.com) is a domain administrator and applications developer for Computer Sciences Corporation.

FEATURE

Moving Exchange to the Cloud, Part 2

Consider the costs before making the leap

by Tony Redmond

In "Moving Exchange to the Cloud, Part 1" (January 2010, InstantDoc ID 103110), I discussed the changing competitive landscape for Microsoft Exchange Server and the engineering effort in Exchange Server 2010 to create a version of the software that is suitable for cloud-based deployments as part of Microsoft's Business Productivity Online Standard Suite (BPOS). In this article I discuss some of the challenges companies face as they determine whether cloud-based services are suitable for their purposes.

Companies that are considering moving their Exchange-based email services to the cloud have many things to consider. Some companies are ahead of the game, because they're already using the Internet to replace expensive dedicated connections between their company network and a hosting provider. By exploring their own variation of the cloud, they can better understand the challenges they will face if they truly move to cloud-based services. Other companies might never transition from in-house servers because of their overall conservative approach to IT, fears about data integrity, regulatory or legal compliance requirements within certain industries (e.g., the FDA requirement to validate the systems that pharmaceutical companies use for drug trials), the unavailability of high-quality or sufficient bandwidth in certain geographic locations, or because they operate in countries that require data to stay within national boundaries. Some companies might be chomping at the bit to move to Microsoft Online Services because they're running older versions of Exchange Server and they see cloud computing as an effective way to upgrade their infrastructure.

Regardless of how eager (or reluctant) your company might seem to embrace cloud computing, you need to ask several questions to evaluate whether your organization is truly ready to operate email in the cloud. You need to consider hosted email options, user needs, support responsibilities, application integration, and cost. In addition, you should be aware that hosted email services simply might not be the best solution for your organization.

Hosted Email

BPOS includes two flavors of hosted Exchange: dedicated and standard. The dedicated offering is available only to customers that have at least 5,000 mailboxes—probably because creating a dedicated environment with network, hardware, Help desk, security, and directory synchronization components on any smaller scale than this just isn't worthwhile. The standard offering uses a multi-tenant infrastructure to support mailboxes. All the mailboxes are hosted on the same set of servers and use the same directory (i.e., Global Address List), with logical divisions that make the mailboxes and directory appear to be separate.

Microsoft promises 99.9 percent scheduled uptime for data centers that currently run Exchange Server 2007 with a planned upgrade to Exchange Server 2010. Note that Microsoft already offers Exchange 2010 as a hosted service to customers in the educational sector as part of Exchange Labs; this approach has let the Microsoft development group test and prove the code during Exchange 2010 development to ensure that it's suitable for large-scale hosted deployments.

Standard hosted Exchange offers several add-ons for an additional cost; these options include a mailbox capacity upgrade from the base 1GB, BlackBerry support, archiving, and migration from another email system. The standard offering supports Windows Mobile 6.0 and later devices, Outlook 2007, Outlook 2003, Outlook Web Access (OWA), and Entourage; it will also support Outlook 2010.

The dedicated offering is more flexible and customizable, because it's committed to just one customer. This service includes options such as business continuity and disaster recovery.

List prices vary from country to country. Microsoft announced in November 2009 that it would offer BPOS for $10 per user per month (including Exchange, SharePoint, and Office Communications Server—OCS). The price reduction was intended to allow Microsoft to compete head-to-head with Google Apps Premier Edition, which starts at $50 per user per year plus add-ons. However, the new price came as a shock to many hosting partners because it makes a substantial cut in the margins available in the hosting business. The price war between Microsoft and Google will continue and might further lower mailbox costs.

Because Microsoft designed Exchange 2007 for traditional deployments, it isn't surprising that some of the more advanced features such as transport rules, rights management, and unified messaging (UM) don't work in hosted environments. Microsoft expects to be able to support these features in Exchange 2010 because this version was engineered to support multi-tenanted hosted deployments. Exchange 2010 also has an improved distributed management model that leverages PowerShell 2.0's remote capabilities to let administrators control their data running on servers in Microsoft data centers.

Before you decide to move email services into the cloud, you should consider whether you have any user groups with special needs that must be met.

Users

Before you decide to move your email services into the cloud, you should consider whether you have any user groups with special needs that must be met. For example, companies often take special measures to ensure the highest degree of confidentiality and service for their most important users, such as executives. They place these users' mailboxes on specific servers that are managed differently than regular systems. Administrative access is limited to a small set of administrators, the servers might be located in different computer rooms, and special operations procedures might apply for backups and high availability. Although you can expect Microsoft to secure data as it moves to and from clients on your network, over the Internet, to servers in Microsoft's data centers, data security will remain a concern as you transition from an in-house system to the cloud—especially in the case of highly confidential data such as that contained in executive email files.

Another issue to consider is how your users work together. For example, can users continue to enjoy delegate access to calendars and other mailbox folders in a mix of in-house and cloud deployment? Or do you have users who need to share data on the same platform? Is the number of calendars that a user can open limited? Do you have shared mailboxes, resource mailboxes, or mailboxes used by applications? These questions don't yet have good answers, because there still isn't a lot of experience in deploying and managing large-scale Exchange organizations that use BPOS. However, these are the types of questions you need to ask to better understand your users' requirements, from basic mailbox access to sophisticated use of advanced Outlook and Exchange Server features.

Simply establishing a service level agreement (SLA) is easy; monitoring end-to-end performance for email and understanding the roles that local and cloud support play are more complicated endeavors.

Support

Negotiating cloud services involves establishing a service level agreement (SLA) that describes the level of availability of the service (e.g., 99.99 percent uptime), explains how the provider will handle outages, and outlines the financial compensation due if the service doesn't meet the contracted uptime. Simply establishing an SLA is easy; monitoring end-to-end performance for email and understanding the roles that local and cloud support play are more complicated endeavors.

Your company provides its own local support, which typically includes the network infrastructure (e.g., connectivity to the Internet, client software, integration with other applications that depend on email). The service provider supports the services it provides. The majority of support activity occurs locally; contact with the service provider is necessary only when the service is unavailable for an extended period (e.g., the August 2008 Google Gmail service outage). Because the Internet connects your network to the

cloud, you can expect transient network hiccups that cause clients to lose connectivity from time to time—after all, no one is responsible for the Internet, and no ISP can guarantee perfect Internet connectivity. (Which, incidentally, is why Cached Exchange Mode is such a valuable Outlook feature.)

Even networks that are under a single company's control still experience problems on occasion. Administrators must understand where local problems are likely to occur and know how to quickly address them, before escalating problems to the service provider. For example, an outage might occur with the provider that connects your network to the Internet, a firewall or router might fail when it becomes overloaded with incoming or outgoing connections, or a systems administration error might block traffic outside your network.

Moving your email to the cloud prevents you from having a full end-to-end picture of the connections between your clients and the mail server, as well as limits your control to only the parts of the network that reside inside your firewall. Users typically hold the local Help desk accountable if they can't access their mailboxes—which creates a difficult situation if the local administrator can't trace the path of a message as it flows from client to server, or can't verify that all the connections are correctly authenticated. In fact, because there are so many moving parts that could fail, including the Internet link, it's difficult to hold a service provider to an SLA unless you have unambiguous proof that the cloud service failed. Experience will prove how easy it is to manage and measure end-to-end service availability in the cloud. For now, there's a weakness in management and monitoring tools, including the ability of these tools to peek inside the cloud data centers, to allow administrators to verify that an SLA is being met.

Applications

Exchange is often integrated with other applications, including Microsoft applications such as SharePoint and OCS, and applications from other major software providers such as SAP and Oracle, as well as home-grown applications built on top of Outlook or Exchange using a variety of APIs ranging from WebDAV to Exchange Web Services. If you move to a cloud-based implementation, you must determine how to handle all your applications that depend on email.

The solution is simple in some cases—for example, online versions of SharePoint and OCS are available as part of BPOS, so you can just replace an in-house implementation with a hosted implementation (assuming that you haven't customized your applications to add elements, such as your own web parts for SharePoint). Moving custom applications into a hosted environment may or may not be possible, depending on what you've actually coded. Unified communications (UC) also poses challenges because of the number of different PBXs and other communications devices in use. The standard delivery provided by an online service might not be able to accommodate your telecommunications infrastructure, in which case you need to continue to run telecommunications in-house or look for another partner who can support your requirements.

Administrators must understand where local problems are likely to occur and know how to quickly address them, before escalating problems to the service provider.

Anyone who has been through a platform upgrade can tell you that the IT department usually underestimates the number of applications in use within a company. Of course the IT department is aware of headline applications that they are responsible for, but they might not know about applications developed by individual users or workgroups that are now part of the business processes. These applications might include Excel worksheets, Access databases, or web-based systems used for various purposes. IT administrators often learn of these applications only when they upgrade the client or server platform and users later complain that their favorite applications no longer work.

In considering Exchange's interaction with applications, you must also consider public folders. Although Microsoft has indicated an intention to eliminate public folders from Exchange since 2003, customer demand has forced the company to commit to public folder support until at least 2016. Some companies have thousands of public folders holding gigabytes of data to archive email discussion groups or store sophisticated workflow applications. Determining how your organization's public folder implementation will function in the cloud can be a complicated process. For example, can a mailbox in the cloud access the contents of a public folder on an in-house server? And if the public folder uses a forms-based application, can that mailbox access the form and load it with the correct data to allow users to interact successfully with the application? It's inconceivable that Microsoft will allow companies to migrate public folders into Exchange Online, because the notion of support for customizable applications runs contrary to the ethos of a service delivered through a utility-based multi-tenant infrastructure—that is, a bounded set of functionality delivered at a low price point, which is achieved on a massive scale only because everyone gets the same service.

The same problem rears its head when you consider aspects of other Microsoft applications, such as Outlook Web Access (OWA) customizations (e.g., changing the logon page to display your corporate logo) or SharePoint web parts that are necessary for an application to run. Utility services are just that—a utility. You wouldn't ask your water company or electric company to provide a custom service, and you likewise shouldn't expect Microsoft to deliver a customized form of Exchange or SharePoint from its utility service. Perhaps in the future Microsoft will allow companies to customize certain aspects of online services, but I don't expect this trend to start anytime soon.

Cost

One of the main advantages of moving into the cloud is reducing your hardware costs, because you'll no longer have to purchase servers and storage for hosting applications. In addition, you'll save money by paying less in software licenses for your servers. Of course, some of your recovered expenses will be offset by the monthly subscription fees you'll be paying for each mailbox. Additional costs might include increasing the size and speed of your network connection to the Internet.

Your initial Internet connection is based on the volume of traffic you expect to generate; that volume will certainly grow if you move your email into the cloud. Mail traffic that previously stayed inside the organization will have to be transported to Microsoft and perhaps back to your network. Directory synchronization and other administrative traffic will make additional demands. In addition, moving mailboxes during migration will tax your network connection's bandwidth. Before you plunge into the cloud, you need to ensure that your network connection can cope with the additional traffic. You might also need to upgrade your infrastructure to handle the increased load of authenticated connections flowing into and out of your company. For example, you might need to upgrade your firewalls, routers, or other network components. In addition, you might need to purchase special software to handle network monitoring and security.

Finally, you need to set aside a budget for all the work necessary to move mailboxes and other data to the hosted service. Basic processing such as directory synchronization is unlikely to cause many problems because it must be done for every hosted implementation, but you might have some special needs. For example, if you have a link-up between Exchange and your HR system so that a mailbox is automatically provisioned when a new employee joins the company, you'll need to validate that this process works with the hosted service. You also need to work through common procedures such as recovering mailbox data from backup to understand how this task will be accomplished with a hosted server. This extra work takes time and effort that you need to budget for.

Contingency Plan

You need to consider the possibility that you could run into problems with a cloud-based implementation and decide to switch back to in-house services. For example, the service might not deliver the functionality that your users require. You might also discover that the service costs more than you expected. Or perhaps your company will be sold to another company that has a successful and cost-effective in-house deployment of Exchange that the new company wants to continue using. Finally, you might just decide that transferring email to Microsoft Online creates a lock-in situation that you aren't happy with.

Regardless of the circumstances, it's a good idea to determine your back-out plan in advance. Consider the different scenarios that could occur over the next five years and outline your response to each scenario. Even though your initial approach might be flawed and incomplete, you'll at least have a starting point for addressing particular problems. In addition, just thinking about how you might retreat from the cloud may very well cause you to rethink how you will enter the cloud in the first place. You might think of possible problems that you need to address in your initial implementation. For example, ask yourself how quickly you'll be able to move mailboxes back to an in-house infrastructure if doing so becomes necessary. Another thing to consider is that although you won't need as many messaging administrators to support a cloud solution once the migration is complete, you might want to retain some of your in-house messaging experts just in case you decide to reverse course, as well as to monitor the hosting provider's delivery to ensure it meets the established SLA.

Although you won't need as many messaging administrators to support a cloud solution once the migration is complete, you might want to retain some of your in-house messaging experts just in case you decide to reverse course, as well as to monitor the hosting provider's delivery to ensure it meets the established SLA.

Future of the Cloud

Cloud services are already here and will play a big role in the future delivery of IT services to end users. The question is how quickly organizations will be able to embrace the cloud and what challenges they'll encounter along the road. The decision to use an online email service will be easy for some organizations, especially those that either don't already have an existing email service or haven't customized their current email service. Moving to a hosted service such as BPOS will also be easier for small companies, whose requirements are typically straightforward and whose financial staff will embrace the prospect of a known cost for mailboxes. Transitioning to the cloud becomes much more complicated the longer an organization has been using email, the more mailboxes the company supports, and the better email is integrated with other applications. In some situations, a standardized online service might simply be too utilitarian to meet your needs, and a more traditional outsourced option (including one that leverages cloud principles to reduce cost) or in-house deployment will be a better solution.

InstantDoc ID 103285

Tony Redmond
(12knocksinna@gmail.com) is a contributing editor for *Windows IT Pro*, and author of *Microsoft Exchange Server 2007 with SP1* (Digital Press).

FEATURE

Quickly Respond to Security Threats with Forefront Threat Management Gateway

Anti-malware, firewall, intrusion detection, and more

by Russell Smith

Microsoft Forefront Threat Management Gateway (TMG) 2010 offers a dynamic response to security threats, providing a variety of security technologies such as anti-malware, firewall, and intrusion detection under one umbrella. It replaces Internet Security and Acceleration Server (ISA) 2006 and integrates with Forefront Protection Manager (currently in beta and due to RTM in Q1 2010), a single-console solution, previously code-named Stirling, which offers central management of Microsoft Forefront products. Forefront TMG connects to Forefront Protection Manager via the Security Assessment Sharing (SAS) system.

Forefront TMG Medium Business Edition was recently released as part of Essential Business Server and is designed to protect up to 300 users. Forefront TMG 2010 Standard and Enterprise editions replace ISA 2006, with the Enterprise Edition supporting deployment and management of TMG arrays and an unlimited number of processors.

Microsoft calls Forefront TMG 2010 a Unified Threat Management (UTM) product, and improvements over ISA include the ability to inspect outbound SSL traffic, definition-based network inspection (NIS), and malware blocking at the gateway. Let's walk through the major features and basic setup of Forefront TMG 2010.

Installing Forefront TMG 2010

Forefront TMG 2010 requires Windows Server 2008 or Windows Server 2008 R2 (64-bit editions only), 2GB of RAM, 2.5 GB of free disk space, and one or more network cards. Additionally, you will need to install the .NET Framework 3.5, Windows PowerShell, and the Microsoft Message Queuing Service with Directory Integration. You can download Forefront TMG 2010 at technet.microsoft.com/en-us/evalcenter/ee423778.aspx. For the purposes of this article, I installed Forefront TMG on a Server 2008 R2 member server with one network card connected to the Internet and another to my internal network.

The Preparation Tool wizard guides you through installation, allowing the selection of required components. You can choose among three options when installing Forefront TMG: Forefront TMG Services and Management, Forefront TMG Management only, and Enterprise Management Server (EMS) for centralized array management. Arrays consist of multiple TMG servers that work in unison to provide high availability and scalability. In this simple testing scenario, I opted for Forefront TMG Services and Management, which installs Forefront TMG and the management console.

Once installed, Forefront TMG offers a series of Getting Started wizards for basic configuration, the most important of which is the Network Settings wizard, which lets you choose the topology for firewall configuration. Setup is unusually fast and simple for a Microsoft server product.

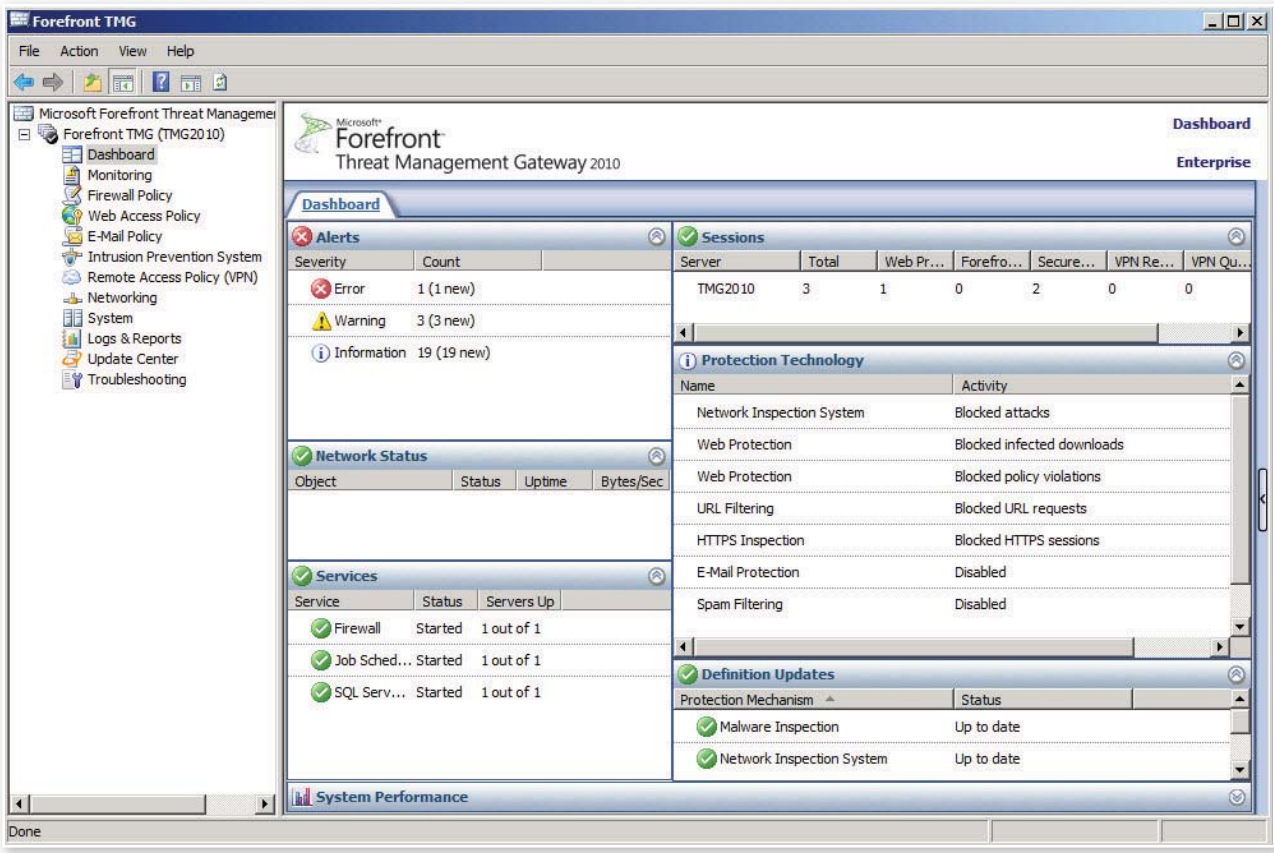


Figure 1: Forefront TMG dashboard

Features in Forefront TMG 2010

Forefront TMG takes ISA beyond firewall, proxy, and remote access, and it provides a comprehensive UTM solution. Forefront TMG boasts the ability to inspect inbound and outbound HTTPS traffic; the ability to block malware downloads at the gateway; an improved network inspection system; and category-based URL filtering for controlling employee Internet access (or "productivity management" in Microsoft-speak).

For the first time, Microsoft's enterprise firewall application runs on 64-bit processors, permitting better performance along with deep network inspection. Another important feature of Forefront TMG is that it integrates with Forefront Protection Manager, currently in beta, which collects data from other products in the Forefront range, letting administrators configure dynamic protection against threats as they're discovered on the network.

Besides the wizards that are launched after setup has completed, the Role Configuration tab on the main Forefront TMG screen provides quick links to various parts of the console so you can continue configuration. However, no additional configuration wizards are provided.

The dashboard and monitoring screens, which Figure 1 shows, provide a good overview of all of Forefront TMG's components, as well as other network services that it depends on, such as Active Directory (AD) and DNS. The Tasks pane on the Firewall Policy node provides quick links to publish common servers such as SharePoint or Exchange Mail services. Forefront TMG is supplied with a Session Initiation Protocol (SIP) filter that automatically manages the opening and closing of Real Time Protocol (RTP) ports for VoIP sessions.

Forefront TMG is supplied with a Session Initiation Protocol (SIP) filter that automatically manages the opening and closing of Real Time Protocol (RTP) ports for VoIP sessions.

Web Access Policy includes proxy authentication, HTTP compression, HTTPS inspection, malware protection, and caching. The category-based URL filtering is based on information provided by Microsoft Reputation Services. Forefront TMG can also be used as an SMTP relay, providing spam filtering and virus protection for Exchange. If installed on the same machine as Exchange Edge Server and Forefront Protection 2010 for Exchange, Forefront TMG can be used to centrally manage SMTP, antispam, and anti-malware policies on the network edge with support for arrays.

Definition-based network inspection in Forefront TMG, which Figure 2, page 58, shows, is based on new technology from Microsoft Research—Generic Application-level Protocol Analyzer (GAPA)—and can be

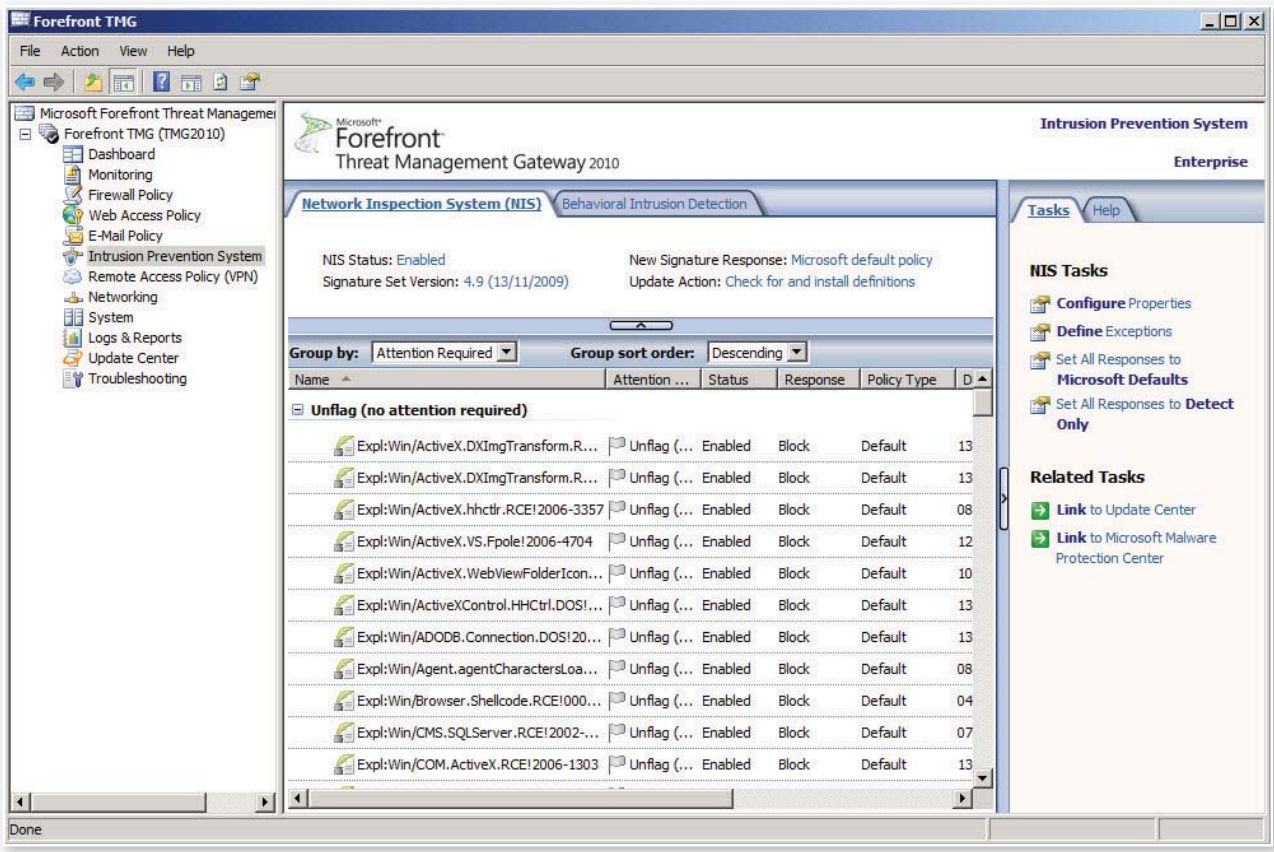


Figure 2: Forefront TMG network inspection

used to block traffic to network resources if an attack pattern is identified. Network inspection, otherwise known as virtual patching, can be useful in situations in which a patch has not yet been developed or deployed for a known vulnerability, especially considering the speed at which a definition can be implemented. Other standard features carried over from ISA 2006 include DNS attack detection and flood mitigation.

Despite the limited focus on new inbound access features in this release, the most important development in TMG Remote Access is support for Server 2008's Network Access Protection (NAP), enforcing health policies when VPN clients connect via TMG and disposing of the complex script-based Network Access Quarantine (NAQ) that shipped with Windows Server 2003. Forefront TMG also adds integrated support for SSTP, allowing Windows Vista and Windows 7 users to make a VPN connection over HTTPS.

ISP redundancy is a great new feature in Forefront TMG for companies that don't want to rely on a single ISP. Not only can Forefront TMG detect when a link is down and move all traffic to a redundant network, load balancing can be performed across links, so that if one link is faster, more traffic can be routed via the faster link.

As in ISA, Forefront TMG's Firewall Client can provide comprehensive reports on user activity and network traffic. The detailed reporting provided by Firewall Client, which is an optional component that can be installed on desktops and notebooks for advanced functionality, proves especially useful in high security environments or for companies that must comply with strict regulatory requirements. Forefront TMG's Firewall Client can be configured to use AD to securely discover approved web proxy servers, as opposed to using the Web Proxy Auto-Discovery Protocol (WPAD), which is less secure and more complicated to set up.

Forefront TMG Will Be a Winner

ISA has always provided the most complete protection for Microsoft products, and Forefront TMG builds on that foundation. Systems administrators will warm to the improvements on the usability front from the outset, such as setup wizards and support for Server 2008's NAP. Another nice touch is the ability to enter a change description and export the current settings before applying configuration changes. With the exception of support for SSTP and secure server publishing features from ISA 2006, going forward, most new inbound access developments will focus on Microsoft's new Forefront Unified Access Gateway (UAG) product. Finally, with the promise of true dynamic infrastructure management, Forefront TMG will integrate with Forefront Protection Manager to provide reactive responses to emerging threats and proactive security.

InstantDoc ID 103278

Russell Smith
(rms45@rsitc.com) is an independent IT consultant. He has been working in IT since 2000, specializing in systems management and security.

Customizing SharePoint Site Templates

by Ron Charity

Boost user productivity via the use of site templates and definitions

Microsoft SharePoint sites are groups of smart web pages in Windows SharePoint Services (WSS) 3.0 and Microsoft Office SharePoint Server (MOSS) 2007 that let users store, manage, and share data via lists and document libraries. Although SharePoint ships with several site templates that simplify site creation, often administrators want to create a custom template so that users can provision sites that meet their specific needs and become productive faster. There are two ways to customize a template: site templates and site definitions. This overview of site templates and site definitions explains the differences between the two methods and walks you through designing, creating, and customizing SharePoint site templates. This is an extensive subject; I've tried to squeeze a lot of information into this article but have barely scratched the surface. I've included references to examples and further reading that will help you dive deeper into the subject.

Site Templates vs. Definitions

A site template is a package that contains a set of differences from a base site definition. Site templates let you use a browser to easily create a template site from an existing SharePoint site. The site, including pages, lists, libraries, and contents, is archived into a single .stp file.

A site definition is a set of files that define the look and feel of a SharePoint site and are stored on the web front-end (WFE) file system in the \12\TEMPLATE\SiteTemplates folder. Creating or modifying site definitions requires programming skills and is far more complicated than using site templates because when creating a site definition, you need to create XML files that describe the site layout and content and package it in a deployment solution.

At some point, most SharePoint administrators will want to change or add certain functionality to the standard site templates. Let's use the example of a proposal in a document management site that requires certain features. These features aren't included in the standard template. So instead of the user creating a site using the standard document management template and manually customizing the site, he or she can simply use a custom template that has already been created for proposal management.

Site Templates and Site Definitions: Which Should You Use?

How do you choose between site templates and site definitions when customizing a template? Let's look at some of the pros and cons of each method. The more you understand about the two techniques, the better you'll be able to determine the best method for customizing your sites.

Site template pros. Site templates let administrators create predefined sites to simplify site provisioning from a user perspective. Sites that are created with templates are consistent, which improves usability and maintenance. The pages are stored in just one location—the content database.

Site template cons. Because the pages are stored in the content database, performance degradation could occur. Once you create and save a template, you can't update it, which might lead to future product compatibility issues.

Site definition pros. Administrators must programmatically create site definitions, giving them more control over site creation. Sites can be provisioned easily—users don't have to customize them. Site definitions provide greater control over a site's look and feel. Because sites are more consistent, there are fewer user support calls for help.

Site definition cons. Creating site definitions requires programming skills (i.e., Visual Studio). Site definitions are costly to maintain. The definition files are stored on each WFE server; therefore, updates must follow change control management processes when multiple WFE servers are involved.

Designing Sites

Many SharePoint administrators think that to create a site, you simply open a template, create some web parts and any needed columns, set up security, and you're done. But you and your users will likely be disappointed if you don't take the time to design a site that provides the functionality to meet the needs of the users. For example, the first step in the design process is to meet with the users to:

- Understand the tasks or job the site will facilitate and support. This will give you insight regarding functionality (their wish list), and its value as mapped to their jobs (business need).
- Identify the web parts required and whether custom web parts or features are required.
- Understand the lingo they use in the job activities and tasks related to the site. This will help you understand how to label the site, web parts, columns, and views, so that they make sense to the user.

Table 1: Web Parts for Sample Site

Web Part Name	Web Part Type	Location	Custom Columns
New RFP Content To Be Reviewed	Document library	Middle column	RFP Section
Announcements	Announcements	Middle column	
Latest RFP Content Reviewed and Published	Document library	Right column	RFP Section
Bid Team Contacts	Contact list	Right column	Bid Team Role
Links to Materials	Links	Right column	
Bid Team Discussions	Discussion library	Middle column	Section of RFP
RFP Questions	Custom list	Middle column	Question Section Author Answered
Calendar	Calendar	Not shown on main page	

Creating Site Templates

The first step in creating a site template is to create the site that will be a base for your template. Note that site templates are created using the SharePoint standard Site Actions pages—Visual Studio isn't required. This section assumes that you're familiar with adding sites and web parts and adding or modifying columns.

To create your site, open a browser, enter the URL to your SharePoint server, and follow these steps:

1. Select Site Actions, Manage Hierarchy. Right-click the area in the site hierarchy where you want to create a site, and select Add Site.
2. When prompted for a site name, enter TemplateSite, and for the URL, enter TemplateSite, as Figure 1 shows. Select a site template (in our example, Team Site) and click OK. Make note of the URL because it's required for the next step.
3. To customize the site, enter the site's URL, press Enter, and wait for the site to load. Select Site Action and choose Edit Page. Add the web parts listed in Table 1 to the page. To learn how to add web parts, see the Microsoft article "Add or remove Web Parts from a page" (office.microsoft.com/en-us/sharepointserver/HA011605831033.aspx). Figure 2 shows the site in its completed form.
4. To save the site as a template, enter the URL of your site, press Enter, and wait for the site to load. Select Site Action, and choose Site Settings. Under *Look and Feel,* click *Save Site as Template.* On the *Save Site as Template* page in the File Name section, enter TemplateSite. Then select the Include Content check box, and click OK. Note the site template name.
5. To use the template, enter the URL to the provision site (web page). Select *Create a New Site.* You're then prompted to enter a site name, URL, and description.
6. At the bottom of the page, you're prompted for the site template. Here you have the option to select one of the Template SharePoint sites. Select the custom site template you created and continue answering the remaining prompts.

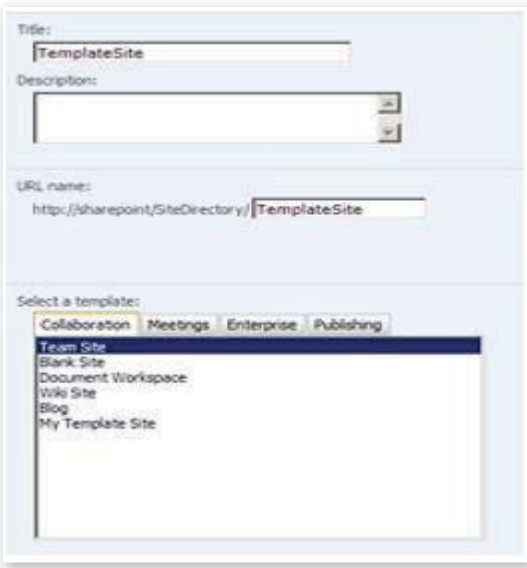


Figure 1: Creating a SharePoint site

Site Definitions

A site definition, as mentioned earlier, is a group of configuration files that provide a framework for creating SharePoint sites with a certain structure and functionality. Each site definition is contained in its own folder in Local_Drive:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\12\TEMPLATE\SiteTemplates. The file that contains the site definition is onet.xml, which is located in a subfolder called \TEMPLATE\SiteTemplates\SMS\XML\ONET.XML. The following sections describe the key configuration files for site definitions and provide

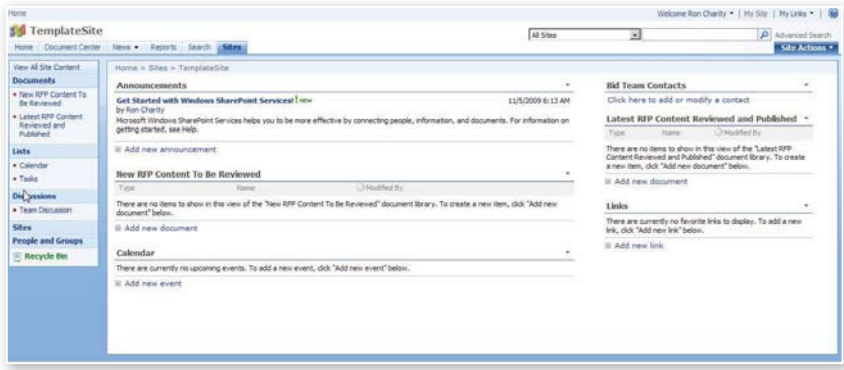


Figure 2: A completed site template

Listing 1: Sample Webtemp.xml File

```
<Templates
  xmlns:ows="Microsoft SharePoint">
  <Template
    Name="STS"
    ID="1">
    <Configuration
      ID="0"
      Title="Team Site"
      Hidden="FALSE"
      ImageUrl="/_layouts/images/stsprev.png"
      Description="A site for teams to quickly
        organize, author, and share information.
        It provides a document library, and lists for
        managing announcements, calendar items, tasks,
        and discussions."
      DisplayCategory="Collaboration" />
    <Configuration
      ID="2"
      Title="Document Workspace"
      Hidden="FALSE"
      ImageUrl="/_layouts/images/dwsprev.png"
      Description="A site for colleagues to work
        together on a document. It provides a
        document library for storing the primary
        document and supporting files, a tasks list
        for assigning to-do items, and a links list
        for resources related to the document."
      DisplayCategory="Collaboration" />
  </Template>
  <Template
    Name="MPS"
    ID="2">
    <Configuration
      ID="0"
      Title="Basic Meeting Workspace"
      Hidden="FALSE"
      ImageUrl="/_layouts/images/mwsprev.png"
      Description="All the basics to plan, organize
        and track your meeting. This Meeting Workspace
        contains the following lists: Objectives,
        Attendees, Agenda, and Document Library."
      DisplayCategory="Meetings" />
  </Template>
</Templates>
```

examples of how to create a definition and make simple edits to customize it.

Create a Definition

The first step is to create a definition you can work with by copying an existing site definition. To do so, open Windows Explorer and browse to Local_Drive:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\12\TEMPLATE\SiteTemplates. Create a folder called MYCUSTOMSITE. Copy the STS folder contents to the MYTEMPLATESITE.

Webtemp.xml

The Webtemp.xml file determines how site definitions are listed in the different controls that SharePoint uses to create new site collections and subsites (I call it a master list of site templates). This file is located in a language-specific folder in the 12 hive: \12\TEMPLATE\1033\XML\ for English. SharePoint will merge any file that starts with Webtemp into one list of available site definitions.

Each WFE server in a SharePoint deployment (both WSS 3.0 and MOSS 2007) has at least the originally installed Webtemp.xml file located in the Local_Drive:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\12\TEMPLATE\LCID\XML folder, where LCID is the numeric ID of the language/culture (e.g., 1033 for English). There may also be one or more custom Webtemp*.xml files. The Webtemp*.xml files contain the site definition configurations that are available on the Template Selection section of the New SharePoint Site page. Listing 1 shows a sample Webtemp.xml file.

Each site definition is identified by a name and a unique ID. If your ID isn't unique across the farm, you'll receive invalid template errors. I usually work in a range far away from the standard Microsoft IDs (e.g., 2002, 2003). You also need to maintain a central registry list (e.g., in your project SharePoint site) of all the IDs that you have used in your customer project.

I could add a custom site by inserting the following lines of XML within the Template element:

```
<Template
  Name="MYTEMPLATESITE"
  ID="2002">
  <Configuration
   ID="0"
   Title="My Template Site"
   Hidden="FALSE"
   ImageUrl="/_layouts/images/
     mwsprev.png"
   Description="Description of my
     template site."
   DisplayCategory="Collaboration" />
</Template>
```

Note that the Name must be upper case (i.e., MYTEMPLATESITE). Close your browser and run IISRESET from the command prompt. (This will make sure SharePoint is working with the new XML file.) You can now work with your new template by experimenting with making changes and edits.

Onet.xml

The onet.xml file provides the content (web parts) and layout of a site definition. (I call it a master description.) Microsoft's official description is that in an onet.xml file, the Feature element is used within a site definition configuration to contain a reference to a Feature instance and default property values. The Configuration element specifies lists and modules to use when creating SharePoint sites (msdn.microsoft.com/en-us/library/ms474369.aspx).

Use caution when working with onet.xml. Don't modify the contents of the global onet.xml file (\TEMPLATE\GLOBAL\XML), because doing so can break the installation. The onet.xml file contains site definitions for the following elements:

- NavBars—The navigation bars on team site pages
- ListTemplates—The possible lists and document libraries for the site
- DocumentTemplates—Document library templates available for the site
- BaseTypes—Base lists and definitions of the fields contained in a site

- Configurations—Defines instances of lists and libraries created and contains pointers to modules
- Modules—Modules define per ASP.NET page the web parts that need to be displayed

To begin, let's look at the NavBars element in the onet.xml file:

```
<NavBar Name="SharePoint Top Navbar"
   Separator="   "
  Body="<a ID='onettopnavbar#LABEL_ID#'
   href='#URL#' accesskey='J'>#LABEL#</a>"
   ID="1002">
  <NavBarLink Name="Documents and Lists"
     Url="viewlsts.aspx" />
  <NavBarLink Name="Create"
   Url="create.aspx" />
  <NavBarLink Name="Site Settings"
   Url="settings.aspx" />
  <NavBarLink Name="Help" Url="javascript
     :HelpWindowKey("helphome")" />
</NavBar>
```

I could add a link to Google by inserting the following lines of XML code within the NavBar element:

```
<NavBarLink Name="Google"
  Url="http://www.google.com">
</NavBarLink>
```

The ListTemplates section defines the lists and libraries you can make available within your site definition. Note that the ListTemplates section isn't included in the onet.xml file of the standard SharePoint site definition, which instead uses list definition Features and element .xml files to define its list templates. The example that Listing 2 shows is taken from the onet.xml file.

DocumentTemplates

The DocumentTemplates section defines the document templates that are listed on the new page. It also contains the collection of document library templates that are available for creating document libraries. This collection is listed in the Template Type drop-down list box on the New Document Library page.

```
<DocumentTemplates>
  <DocumentTemplate
    Path="STS"
    DisplayName="$Resources:core,
      doctemp_Word;"
    Type="121"
    Default="TRUE"
    Description="$Resources:core,
      doctemp_Word_Desc;">
    <DocumentTemplateFiles>
      <DocumentTemplateFile
        Name="doctemp\word\wdtmpl.dotx"
        TargetName="Forms/template.dotx"
        Default="TRUE" />
    </DocumentTemplateFiles>
  </DocumentTemplate>
  ...
</DocumentTemplates>
```

You could edit this <DocumentTemplateFile /> tag to include a custom template such as CustomerOrder.dotx:

```
<DocumentTemplateFile
Name="doctemp\word\CustomerOrder.dotx"
TargetName="Forms/CustomerOrder.dotx"
Default="TRUE" />
```

Note that you must replace the template .dotx in the forms directory with your new template.

BaseTypes

The BaseType element of the global onet.xml file is used during site or list creation to define the five list types on which all list definitions in SharePoint are based. Each list template that is specified in the ListTemplate section is identified with one of the following base types: Generic List, Document Library, Discussion Forum, Vote or Survey, or Issues List. Listing 3 shows the code for the BaseTypes element.

Configurations

Each Configuration element in the Configurations section, which Listing 4 shows, specifies the lists and modules that are created by default when the site definition configuration is instantiated. For instance, one configuration can determine the layout of a site when created as a root of a site collection, and another configuration in the same onet.xml file can provide the contents and page layout of a new site when it's created as a subsite in a site collection. For more information, see the article "Configuration Element (Site)" at msdn.microsoft.com/en-us/library/ms476942.aspx.

Features Overview and Example

With WSS 3.0 and MOSS 2007, Microsoft introduced Features. Essentially, Features enable you to add new functionality to SharePoint or make site customizations in an easy and consistent way. The Features framework enables you to scope features at the farm, web application, site, and web level, depending on the purpose of your feature. A feature is implemented using a feature.xml file. The following is an example of a feature file that I created in Visual Studio that adds a link to the tool bar:

```
<?xml version="1.0 encoding="utf-8" ?>
<Feature xmlns=http://schemas
    .microsoft.com/sharepoint/"
  Id="Simple Link"
  Title="MySite Link"
  Description="Add link to toolbar menu
    for MySite"
  Scope="Web"
  Hidden="FALSE"
  AlwaysForceInstall="TRUE">
  <ElementManifests>
   <ElementManifest location="toolbar
     .xml" />
</ElementManifests>
```

Listing 2: The ListTemplates Section from the onet.xml File

```
<ListTemplates>
  <ListTemplate
    Name="meetings"
    DisplayName="$Resources:xml_onet_mwsidmeetingDisp;"
    Type="200"
    BaseType="0"
    Unique="TRUE"
    Hidden="TRUE"
    HiddenList="TRUE"
    DontSaveInTemplate="TRUE"
    SecurityBits="11"
    Description="$Resources:xml_onet_mwsidmeetingDesc;"
    Image="/_layouts/images/itevent.gif">
  </ListTemplate>
  <ListTemplate
    Name="agenda"
    DisplayName="$Resources:xml_onet_mwsidagendaDisp;"
    Type="201"
    BaseType="0"
    FolderCreation="FALSE"
    DisallowContentTypes="TRUE"
    SecurityBits="11"
    Description="$Resources:xml_onet_mwsidagendaDesc"
    Image="/_layouts/images/itagnda.gif">
  </ListTemplate>
    ...
</ListTemplates>
```

Listing 3: The BaseTypes Section of onet.xml

```
<BaseTypes>
  <BaseType
    Title="Generic List"
    Image="/_layouts/images/itgen.gif"
    Type="0">
      <MetaData>
        <Fields>
          <Field
            ID="{1d22ea11-1e32-424e-89ab-9fedbadb6ce1}"
            ColName="tp_ID"
            RowOrdinal="0"
            ReadOnly="TRUE"
            Type="Counter"
            Name="ID"
            PrimaryKey="TRUE"
            DisplayName="$Resources:core,ID"
            SourceID="http://schemas.microsoft.com/sharepoint/v3"
            StaticName="ID">
          </Field>
          <Field
            ID="{03e45e84-1992-4d42-9116-26f756012634}"
            RowOrdinal="0"
            Type="ContentTypeId"
            Sealed="TRUE"
            ReadOnly="TRUE"
            Hidden="TRUE"
            DisplayName="$Resources:core,Content_Type_ID;"
            Name="ContentTypeId"
            DisplaceOnUpgrade="TRUE"
            SourceID="http://schemas.microsoft.com/sharepoint/v3"
            StaticName="ContentTypeId"
            ColName="tp_ContentTypeId">
          </Field>
          ...
        </Fields>
      </MetaData>
  </BaseType>
  ...
</BaseTypes>
```

Listing 4: The Configurations Section of onet.xml

```
<Configurations>
  ...
  <Configuration
    ID="0"
    Name="Default">
    <Lists>
      <List
        FeatureId="00BFEA71-E717-4E80-AA17-D0C71B360101"
        Type="101"
        Title="$Resources:core,shareddocuments_Title;"
        Url="$Resources:core,shareddocuments_Folder;"
QuickLaunchUrl="$Resources:core,shareddocuments_Folder;/
    Forms/AllItems.aspx" />
        ...
    </Lists>
    <Modules>
      <Module
        Name="Default" />
    </Modules>
    <SiteFeatures>
      <Feature
        ID="00BFEA71-1C5E-4A24-B310-BA51C3EB7A57" />
      <Feature
        ID="FDE5D850-671E-4143-950A-87B473922DC7" />
    </SiteFeatures>
    <WebFeatures>
      <Feature
        ID="00BFEA71-4EA5-48D4-A4AD-7EA5C011ABE5" />
      <Feature
        ID="F41CC668-37E5-4743-B4A8-74D1DB3FD8A4" />
    </WebFeatures>
  </Configuration>
  ...
</Configurations>
```

Open Visual Studio and paste this code to a file. Save the file to C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\12\TEMPLATE\FEATURES\MySiteToolBar\Feature.xml.

The following code is the toolbar.xml file that adds a link to MySite:

```
<Elements xmlns="http://schemas
    .microsoft.com/sharepoint/">
 <CustomAction  Title="My Site"
  Id="MySite Toolbar "
  Sequence="10"
  RegistrationType="List"
  RegistrationType="101"
  Description="Add a MySite link to
    the tool bar. " >
   <UrlAction Url="/_layouts/myssite
    .aspx"/>
 </CustomAction>
</Elements>
```

Next, save the file to C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\12\TEMPLATE\FEATURES\MySiteToolBar\ToolBar.xml. Once you've created the feature, you install it using Stsadm. Here is the syntax:

```
Stsadm.exe –o installfeature
  -filename c:\features\Toolbar\
  Feature.xml
```

After you complete the installation, you activate the feature by opening your browser and entering the URL for your portal. Click Site Actions, Site Settings, then under Site Administration, click the Site Features link. Look for your feature and click the Activate button. An alternative approach would be to use Sysadm, with the following syntax:

```
C:\Program Files\Common Files\Microsoft
  Shared\Web Server Extensions\12\bin\
  stsadm -o activatefeature –filename
  MySiteToolBar\Feature.xml -url
  http://ServerName/Sitecollection
```

MSDN provides a lab, "How to: Add Actions to the User Interface," that shows how to create a feature that steps you through adding functionality to the menus of the UI in WSS. The example shows how to add actions to various menus by using a feature and how to activate the actions within the deployment. I suggest you do this lab and create your Site Template to get a sense of the Feature framework and its power. View the lab at msdn.microsoft.com/en-us/library/ms473643.aspx. Two other articles, "Features for SharePoint" (msdn.microsoft.com/en-us/magazine/cc163428.aspx) and "Working with Features" (msdn.microsoft.com/en-us/library/ms460318.aspx), provide further information about using features.

It's All About Usability

Site templates and site definitions can help your organization boost SharePoint usability by creating sites with a consistent look and feel, which helps reduce training and support costs. They also provide an approach for designing site templates that support business requirements and will help reduce the time required to deploy sites. Using the Features framework, your organization can deploy features to sites globally or to specific sites to add functionality and improve user experience.

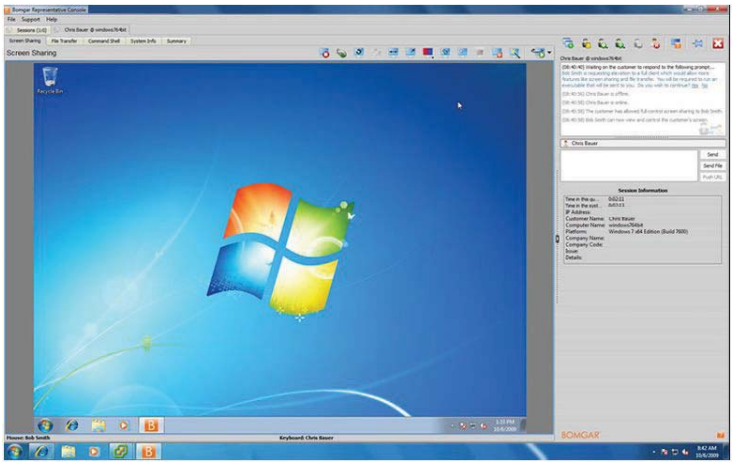
InstantDoc ID 103277

Ron Charity
(ron.charity@hp.com) is an HP solution architect with 20 years of experience. He's located in Toronto, where he focuses on solutions for document and records management, collaboration, search, portals, and social networking.

- Bomgar
- VMware
- DeskCenter
- NewSoftwares.net
- Sherpa Software
- Kerio Technologies

Bomgar Updates Remote Control Software

Bomgar announces **Bomgar 10.4,** a new release that adds support for Windows 7 and expands support for Linux and Mac machines. It also adds a feature called "Rep Invite" that allows Help desk staff to invite someone, inside or outside the company, to share the screen view of the computer in question. According to the vendor, the transition to Windows 7 will likely cause an increase in the need for IT support software—even though Windows 7 is a solid OS, the change from the eight-year-old WIndows XP OS will cause some problems, or at least questions, from users. Bomgar said an increase in users who travel with computers or work from home has also increased the need for Help desk software. To learn more, visit www.bomgar.com.



VMware View 4 Doubles VMs per Core

The latest version of VMware's desktop-virtualization software, **View 4,** has been announced. View 4 includes several new features, including a new protocol that dynamically adjusts to provide a high-quality experience for virtual desktops delivered over a LAN, and an optimized experience over slower WAN connections. It also boasts a big reduction in system requirements. According to the vendor, virtual desktop software could historically provide six to eight virtual machines (VMs) per server core, but View 4 can provide as many as 16. View 4 supports both thin clients and full PCs to provide virtual desktops. Visit www.vmware.com/view.

PRODUCT SPOTLIGHT

DeskCenter Management Suite

DeskCenter Brings SMB Systems Management to United States

DeskCenter Management Suite, a systems management tool aimed at small-to-midsized businesses (SMBs), is now available. The suite offers fast, easy installation and scalable pricing to appeal to businesses as small as 25 users.

The suite offers the functions you'd expect in a systems management utility, including discovery, inventory, OS deployment, software distribution, and patch management. According to DeskCenter representatives, the applications in the suite are as easy to use as Windows Explorer and have such a small installation footprint that they can be installed on a laptop.

Where DeskCenter really aims to stand out is its pricing. The product can scale up to large deployments, but the company is focused on SMBs. The suite boasts a $3,000-$15,000 price tag for deployments of 25 to 250 users, so DeskCenter is hoping it will be adopted in places such as law and medical offices that don't usually deploy systems management products but that could use their features. DeskCenter also offers the suite as a service, so if you have a short-term need for a task such as inventorying a network, there's no need to make a long-term commitment.

DeskCenter Management Suite is certified to manage and deploy Windows 7 and can work with virtual machines (VMs). More information and a trial of the suite are available at www.deskcenter.net.

Protect Data on Your Computer and USB Devices

NewSoftwares.net announces the release of **Folder Lock 6.3.1,** a security program that protects files and folders on your PC and external data devices. Folder Lock lets you lock, hide, and encrypt files—it can also be used to shred sensitive files so they can't be recovered. New features in 6.3.1 include improvements to the UI. Folder Lock costs $39.95, and a free evaluation version is available at www.newsoftwares.net.

Compare Excel Spreadsheets

HigherData has released **Workbook Compare Pro 2.7,** an application that lets you compare two Microsoft Excel spreadsheets and produce a report of the differences. During analysis, Workbook Compare Pro doesn't modify the data on your spreadsheets. Workbook Compare

Workbook Compare - 4/21/09 10:42 PM
9 differences found. (Differences +/- 0 are omitted).
Formula cells were evaluated as values. Double-click a value to navigate to the cell address in the source.

Highlight Differences...

Differences Found								Differences		
Each row is a difference								1,000,000.50	% Difference	
Book 1	Book 2	Sheet 1	Sheet 2	Cell 1	Cell 2	Value 1	Value 2	Difference	Value 1 to 2	Value 2 to 1
Mar09.xls	Mar09 Rev.xls	Fund	Fund	C6	C3	$40.50	$41.00	0.50	1.23%	(1.22%)
Mar09.xls	Mar09 Rev.xls	Fund	Fund	D6	D3	$81,000,000.00	$82,000,000.00	1,000,000.00	1.23%	(1.22%)
Mar09.xls	Mar09 Rev.xls	Fund	Fund	E1	F1	Yield	Yield (Modified)			
Mar09.xls	Mar09 Rev.xls	Fund	Fund	E5	F7	0.32	0.3168	(0.00)	(1.00%)	1.01%
Mar09.xls	Mar09 Rev.xls	Fund	Fund		F8		0.17			
Mar09.xls	Mar09 Rev.xls	Fund	Fund		A8		Bottling Water Co			
Mar09.xls	Mar09 Rev.xls	Fund	Fund		B8		26000			
Mar09.xls	Mar09 Rev.xls	Fund	Fund		C8		$54.00			
Mar09.xls	Mar09 Rev.xls	Fund	Fund		D8		$1,404,000.00			

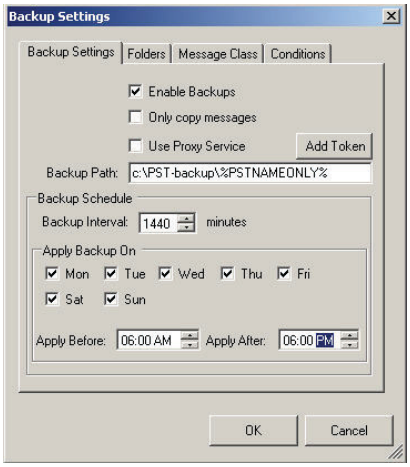
Pro can compare formulas as formulas or as values, and also provides a regression-testing platform. The product costs $69 for a single-user license. A 15-day free trial is also available at www.higherdata.com.

VMware Announces Workstation 7

VMware announces the latest version of VMware Workstation, a product that lets you run multiple OSs on one machine. **VMware Workstation 7** adds Windows 7 support and several new debuggings features. VMware Workstation 6.5 didn't officially support them, but it could already run Windows 7 VMs quite well. In addition to official support for the new OS, VMware Workstation 7 lets you run Windows 7's Aero graphics and other DirectX 3D features. VMware Workstation 7 also adds other features for those who use it for testing. It now supports assigning up to four CPU cores and 32GB of RAM to a VM and allows you to run vSphere and ESXi in VMs. It expands VMware Workstation's Linux support. To learn more, visit www.vmware.com/workstation.

Protect Business-Critical Data with PST Backup Attender

Sherpa Software has announced **PST Backup Attender.** This PST management solution runs on individual enterprise-user desktops and allows systems administrators to quickly and easily back up PST files to a central storage location on the corporate network. PST Backup Attender ensures that email files aren't lost by automatically finding, managing, and backing up PST files, even those that are password-protected. PST Backup Attender extracts data at the individual message level (versus as one large file), so users can retrieve the information they need quickly without restoring entire files. The program can limit the size of



PST files and delete old messages according to IT manager preferences. For more information about PST Backup Attender, visit www.sherpasoftware.com.

Kerio Releases WinRoute Firewall 6.7.1

Kerio Technologies announces the latest release of Kerio WinRoute Firewall. As opposed to a hardware firewall solution that offers no flexibility, Kerio **WinRoute Firewall 6.7.1** lets administrators tailor scalable security solutions, on the hardware or virtualization platform of their choice—the software is available in both a Software Appliance edition and a VMware Virtual Appliance edition (which also integrates with other virtualization platforms). The product is an excellent fit for SMBs that don't have full-time IT departments. The Virtualization Appliance edition is a benefit for SMBs that are already looking to virtualize their file servers or mail servers. Virtualization saves money (server consolidation), environmental resources ("green" computing), and time (faster/easier IT administration). WinRoute Firewall 6.7.1 costs $329 for 10 users. To learn more, visit www.kerio.com.

Paul's Picks

www.winsupersite.com

SUMMARIES of in-depth product reviews on Paul Thurrott's SuperSite for Windows

Internet Explorer 9 Preview

PROS: Microsoft is finally addressing standards support and performance issues from IE 8

CONS: It's too early to tell whether this browser will be better

RATING: n/a

RECOMMENDATION: While Microsoft won't show off a usable version of its next web browser, IE 9, until the MIX conference in March 2010, the company did provide a very early preview in late 2009. And while we have no hints about where Microsoft is going with IE 9's UI, what we did see is heartening: The company is going to focus on performance—real-world performance, not just for benchmarks—better standards support, and, interestingly, hardware-accelerated rendering. If Microsoft can make good on its performance and standards support, the company will go a long way toward fixing the big customer complaints from IE 8.

CONTACT: Microsoft • 800-426-9400 • www.microsoft.com

DISCUSSION: www.winsupersite.com/live/ie9_preview.asp

OFFICE 2010 Starter Edition

PROS: A free version of Office with basic Word and Excel functionality that will meet the needs of many users

CONS: Advertising-supported; utilizes the old Office 2007 UI; can't access crucial Word or Excel functionality

RATING: ◆◆◆◆◇

RECOMMENDATION: Office 2010 Starter edition includes only basic versions of Word and Excel and will replace Microsoft Works. It will be provided only to customers who purchase new PCs. It's advertising supported and features a simplified version of the standard ribbon UI. But the big deal is that Office 2010 Starter is absolutely free and unless you need some crucial but advanced features (like reviewing from Word), it will likely meet most of your needs. Best of all, you can electronically upgrade to a more capable version. The final version is due in June 2010.

CONTACT: Microsoft • 800-426-9400 • www.microsoft.com

DISCUSSION: www.winsupersite.com/office/o2010_beta_starter.asp

InstantDoc ID 103274

Mimosa NearPoint for Microsoft Exchange

In 1964, Bob Dylan sang "The Times They Are a-Changin'." In the world of email archiving and recovery, that seems to be a fitting comment for the present. With a greater emphasis on e-discovery than ever before, solutions that provide disaster recovery and archiving are reinventing what it means to capture your Microsoft Exchange Server infrastructure safely. Mimosa NearPoint for Exchange is one of the industry's leading email archiving solutions for information management, and it boasts an impressive feature set that I found somewhat overwhelming.

Installation and Documentation

NearPoint supports Exchange Server 2010/2007/2003/2000. The setup documentation was clear in outlining how to install NearPoint. I set up a member server on a box separate from my Exchange servers and installed Microsoft SQL Server; you can use SQL Server 2008 or SQL Server 2005, but not SQL Server Express Edition because of database size limitations that could hurt you in the long run. After the prerequisites were in place, it took me less than 30 minutes to perform the full installation, including databases and the Index Object Repository (IOR), and begin managing servers and archiving data. The install was easy, requiring only enough SQL Server knowledge to install and set up an account, which you'll need for creating the databases NearPoint uses.

The documentation provides step-by-step guides for both configuration and installation, and the installation wizard double-checks your prerequisites before installation. The wizard also has a nice feature for the database creation—it asks you to pick an estimated average size for your Exchange mailboxes so the databases can be sized automatically to match the need for the archive. The IOR is configured to hold attachments and such outside of Exchange and it's good to remember this point when the time comes to prepare for a backup/recovery solution of NearPoint. You're going to need both a SQL Server backup and a file backup of the flat-file IOR that is saved.

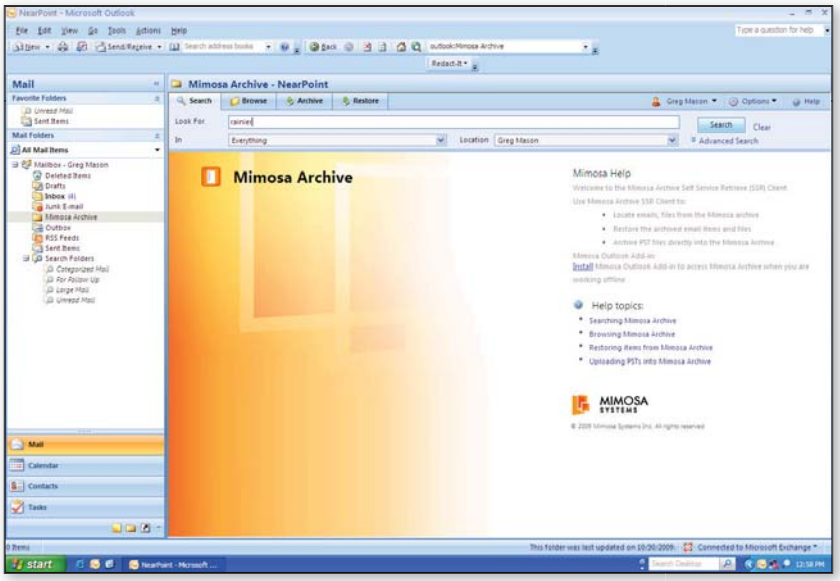


Figure 1: Mimosa NearPoint integration with Outlook

Performance

NearPoint for Exchange doesn't require an agent installed on the Exchange server. It's difficult to test NearPoint's effect on Exchange performance in a lab environment, so I spoke with Andrew Gahm of South Jersey Healthcare, who's been using NearPoint for several years. He verified that he doesn't see a performance hit against his production Exchange environment when working with NearPoint. Personally, I attribute the lack of a performance hit to the method NearPoint uses to capture and crawl.

During installation, the wizard finds your Exchange servers. Once you begin managing the servers, NearPoint begins archiving. The solution itself mimics the high availability options in Exchange 2007 that use continuous replication. NearPoint makes an initial copy of the database and then keeps it up to date using Continuous Application Shadowing. This technology captures transaction logs when they're shipped over, then replays the logs into the database itself.

NearPoint takes that shadowed copy and crawls through the database, allowing it to provide a granular restoration structure and an e-discovery catalog. The result is a point-and-click recovery solution that lets you recover at the database, mailbox, or message level (and more). NearPoint captures, crawls, and then indexes the complete set of Exchange mailbox information, including mail, contacts, calendars, and personal folders, which allows for a great deal of granularity for restoring and e-discovery. During the extraction process, individual messages are broken down into major components (header, body, attachment). Each component is indexed and deduplicated, providing single-instancing and reducing storage costs. All metadata from the message is preserved, including permissions, flags, and context information for folders, as well as some very important information from a legal perspective: whether the email was opened, edited, replied to, forwarded, or deleted.

In addition to the ability to provide continuous application shadowing, NearPoint can also use Microsoft Volume Shadow Copy Service (VSS) captures for log shipping and can read from the passive node of a CCR cluster, eliminating any contact with the active Exchange server. MAPI captures of specific mailboxes are

J. Peter Bruzzese | peter@trainsignal.com

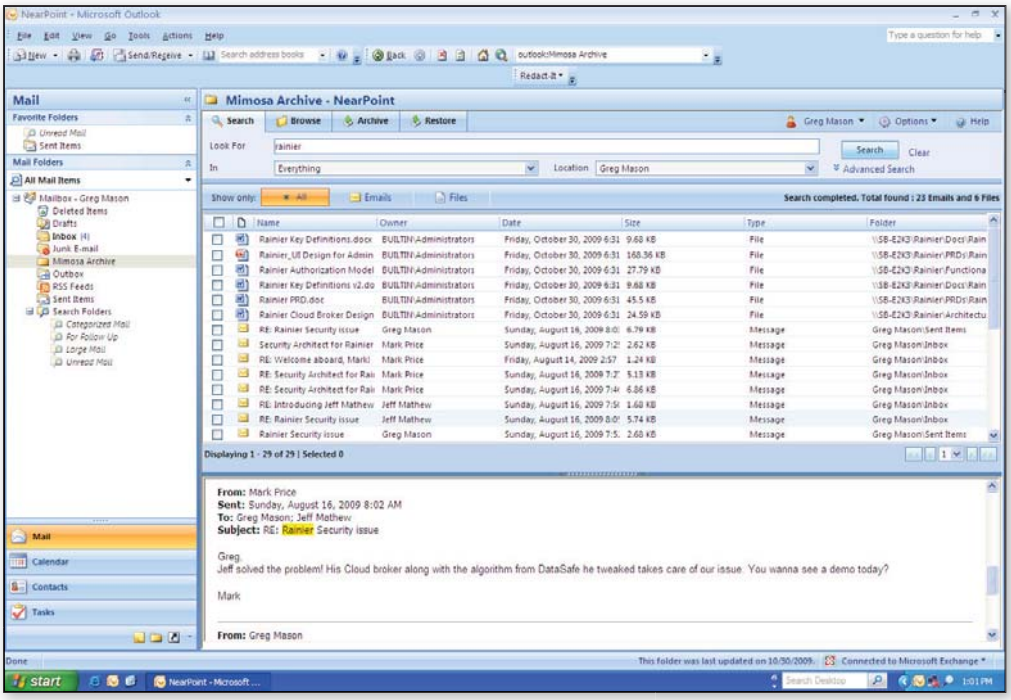


Figure 2: Mimosa NearPoint archive client search results

also possible (rather than shadowing an entire database), even from remote servers.

End-User Self-Service and E-Discovery

One of the features I especially liked was NearPoint's end-user Self-Service Access feature, shown in Figure 1, which allows NearPoint's web-based interface to integrate seamlessly with Outlook or Outlook Web Access. This interface lets users access their archived data and restore it to the Exchange server if necessary. Because the data is full-text indexed, users can search for items no matter where they're stored, as Figure 2 shows.

NearPoint can help reduce Exchange storage using policies that provide stub files that replace actual messages if certain criteria, such as message size or age, are met under the policy. NearPoint replaces messages that meet the criteria with a file that points to the message, which resides on the NearPoint server.

Going beyond what standard users might do with the archive access and recovery, NearPoint provides an e-discovery solution that allows for full legal compliance. It meets all the standard legislative requirements for email, including HIPAA, SOX, SEC Rule 17a-4 and FRCP 34 (b). NearPoint also lets you manage the lifecycle of your corporate email fully. It can define retention time parameters and search through the full capture of data, metadata, and item history, all located in the central IOR. Some of my favorite e-discovery features include the ability to export your search results to a portable format (such as a PST file for external counsel review or court-ready production), the ability to locate BCCs, and the ability to search within a search.

NearPoint's comprehensive list of features for Exchange isn't as available on other platforms, such as Novell GroupWise and Lotus Notes. It works with the other platforms but doesn't have the same level of bells and whistles. NearPoint also isn't a full, end-to-end e-discovery solution—for environments outside of files, SharePoint, and email, companies would need additional products for enterprise-wide e-discovery. For example, structured data search isn't supported.

Times Changin' for the Better

My first two questions for Mimosa were what NearPoint costs and what kind of training Mimosa provides—because people are going to need it. NearPoint costs about $40 per user, with the e-discovery option an additional $16 per seat. As for training, this is enterprise software with the associated risk and time-to-value of a feature-rich product. Although NearPoint is somewhat intuitive and the end-user side is practically a no-brainer, understanding the theory behind some of the retention settings and the best practices for knowing how to use NearPoint properly require some additional training, which Mimosa provides in instructor-led courses. My opinion? Complete thumbs up on this product. I couldn't imagine another feature they could shove into it. It had everything I was looking for and much more.

InstantDoc ID 103333

Mimosa NearPoint for Microsoft Exchange

PROS: Relatively straightforward install; no agent required on the Exchange servers; wide variety of features for archiving and e-discovery.

CONS: Other email platforms aren't supported as thoroughly as Exchange; not a full end-to-end e-discovery solution.

RATING: ◆◆◆◆◇

PRICE: About $40 per user, with the e-discovery option an additional $16 per seat.

RECOMMENDATION: NearPoint's cost might be difficult to justify for smaller environments, and some might categorize it as a convenience rather than a necessity. If you can afford it, however, it makes your life easier. I recommend it as a quality solution for those whose needs (those with stringent legal reporting) and budgets (typically larger environments) allow.

CONTACT: Mimosa Systems • 408-970-9070 • www.mimosasystems.com

Sendio ESP 360

Email spam and malware are serious problems in the business world. IT management of anti-spam systems—not to mention the productivity lost by inadvertently blocking an important message—comes with a significant price tag.

Given the cost and irritation surrounding spam and malware, the market is seeing an ever-growing number of options for dealing with the problem, ranging from hosted solutions in the cloud to software on the mail server. Sendio's E-mail Security Platform (ESP) falls somewhere between those options: It's an appliance that sits on your network in front of your mail servers, protecting them from both spam and malware. The Sendio ESP 360 works on the premise of creating a trusted community of recognized mail contacts. The result, according to Sendio, is zero false positives.

The system doesn't scan content but rather verifies senders. It scans outbound mail for malware and captures details of the receiver, constantly adding those trusted people to the senders' personal mail community. The theory is that you no longer have to maintain complex filters because processing is based on the sender's identity. The system sends unknown senders a challenge query, and—if they respond correctly—adds them to the trusted community.

Setup

The system is reasonably easy to install and configure, and the supplied documentation is excellent. You simply slot the unit into a 1U rack space, attach a monitor and keyboard, and power it up. Initial configuration is keyboard-based, from a clunky Linux GUI on the device console. You must set IP addresses, check for updates, set zone/time sync, and verify that services are running correctly and that the various available communication methods are possible.

After setting up the basics, you open the web-based interface to set up directory sync, which is flexible and worked flawlessly in my test Active Directory (AD) environment. You then jump back to the Linux interface for a few more tasks, and finish off the setup process in the browser interface. Both interfaces are fairly unattractive, and I'm not sure why so much configuration has to be performed from the Linux box's keyboard.

You need to ensure that you import a list of contacts into the device. Administrators can import these as global contacts from a Customer Relationship Management (CRM) system, and end users can use their Microsoft Outlook contacts. If you fail to do this, all your trusted partners and clients will get challenged the first time they send you mail! This process could be challenging for many users who aren't accustomed to importing and exporting from Outlook. Another challenge could simply be gathering a full contacts list. Mine, for example, doesn't contain half the people I mail to. Fortunately, the product's helpful Outlook 2010 Suggested Contacts feature assembles a massive list of people that you've mailed to. Users who have other email systems will find this step difficult.

Results

I tested the Sendio ESP for two weeks, and it successfully ridded my system of all spam. However, it also captured a lot of non-spam mail. There's a significant period required to train the system about the mail you want, by way of releasing that mail from quarantine. The GUI leaves a lot to be desired. It allows no scrolling through its long quarantine list, and certain actions require an inordinate number of clicks. For example, when I double-clicked to review a message and found it to be legitimate, I wanted to be able to simply click Accept. However, I had to go back to the main list, select a check box, then navigate a drop-down list before I could accept that message. Also, there's no immediately discernable way to search the bodies of messages in the quarantine area—only the subject and sender.

A final key criticism: It seems to be impossible to change the challenge message that the product sends to un-trusted senders without calling Sendio support. And the message is natively available only in English and Spanish.

Willing and Able

If you're willing to put in the effort of collating and importing global and personal contacts, Sendio ESP will absolutely make your Inbox cleaner. Initially, though, you'll need to keep a close eye on the notification messages about your quarantine queue and spend a long time in the web GUI. All in all, if you're happy challenging un-trusted senders, and your users can put up with the interface (which is clearly due for an upgrade), the Sendio ESP is a great way to stop spam.

InstantDoc ID 103330

Sendio ESP 360

PROS: Stops spam; supports many mail and directory systems; quality documentation; cluster option

CONS: Clunky GUI; necessity to import contacts and bulk senders you want to receive mail from

RATING: ◆◆◆◆◇

PRICE: $1,995

RECOMMENDATION: If your company is comfortable challenging un-trusted email senders, Sendio ESP 360 is a great way to stop spam.

CONTACT: Sendio • 949-274-4375 • www.sendio.com

Nathan Winters | nathan@clarinathan.co.uk

4 Active Directory Management Tools

Windows Server's Active Directory has evolved into a complex system. These products can help you through the rough spots.

by Eric B. Rux

It's hard to believe that we've been living with Active Directory (AD) for 10 years. If you were in IT during the years preceding this huge paradigm shift, you've witnessed the evolution of how Windows domains are administered. Gone are the days of everyone in IT being a domain administrator. Now, domains can have structure and granular security permissions.

With all that capability, however, came the necessity of forethought and careful planning. If you've ever taken over a poorly planned AD implementation, you understand this necessity all too well. And every day, many administrators face the fact that AD encompasses only one of many user-provisioning tasks. Many companies have Exchange, Research in Motion (RIM) BlackBerry devices, Enterprise Resource Planning (ERP) databases, Human Resources (HR) systems, and countless other systems that users need to have access to. Many of you might also be in the middle of security audits. Sarbanes-Oxley (SOX), Statement on Auditing Standard 70 (SAS70), the Health Insurance Portability and Accountability Act (HIPPA), and other regulatory laws have forced us to rethink how we accomplish daily tasks and how we account for who does them.

Each of the four products in this month's comparative review—**Ensim** Unify Enterprise Edition, **ManageEngine** ADManager Plus, **NetIQ** Directory and Resource Administrator, and **Quest Software** ActiveRoles Server—attempts to take on one or more of these challenges: setting up granular security permissions, user provisioning on multiple systems, and AD auditing. Some try to do everything out of the box, and others use a modular approach.

Test Parameters

To test each product, I ran through five typical administration tasks that the build-in Microsoft tools either don't do or don't do very well. Those tasks are user provisioning (e.g., AD, Exchange, BlackBerry, ERP), Exchange provisioning (e.g., data store based on last name/department), delegation of duties, user de-provisioning a user (e.g., scramble username, reset password, remove from external system), and reporting for audits.

These four products have similar methods for helping you streamline the process of provisioning a new user. If every new user needs to be a member of the ERP Application global group, for example, this feature will be important to you. Another common example of user provisioning is integration with the HR database. Perhaps you'd like AD to be populated with the data from the HR database, or vice versa. Depending on the application, you might need a scripting background to get the most out of this feature.

Ensim Unify Enterprise Edition

Unify Enterprise walks you through a helpful "prerequisite check" for your system, then proceeds through a very simple installation routine. The product runs on Windows Server 2008 or Windows Server 2003 and requires IIS, ASP.NET, .NET Framework 2.0, and the SMTP service. Once the installation is complete, a *Quick Start* guide launches, walking you through some basic steps, such as setting general preferences and notification parameters.

Unify Enterprise has the cleanest GUI of all the products in this review, as you can see in Figure 1, page 70. Through the easy-to-navigate interface, I immediately attempted to create a new user. Doing so led me to want to create a Template User, and in minutes I had nice SpokaneUser and SeattleUser templates. (You can also add users by using a comma separated value—CSV—file.) If your dedicated Help desk staff spends most of its day administering users and computers, this is the interface they'll want to work in.

To help you delegate correct permissions for users, Unify Enterprise includes four built-in roles: System Administrator, Help Desk Administrator, HR Administrator, and Employee. Of course, you can create custom roles, but these four will get you started. For example, the Help Desk Administrator can perform the following tasks: Change and reset passwords, edit user properties, add security groups, and so on.

When a user is deleted from AD, you can set certain events to occur: reset the password to a random string, scramble the logon name, disable the account, move the user object to a special container, and remove the user from all security and/or distribution groups (except for those in an exclusion list). Also, the user's home folder can be automatically archived to another location with the security permissions altered for manager access. The user can then be configured for automatic deletion after a set period of days.

Figure 1: Ensim Unify Enterprise Administrator Enterprise

As for reporting, one of the tabs across the top of the web console is the Reports menu. The following reports are available: Usage, Resource Status, Action Logs, and Deleted Items. Each report is quite detailed, but—from an auditing perspective—I found the most useful information in the Action Logs and Deleted Items. Unfortunately, I couldn't find a way to export the reports into a format that I could give to an auditor.

Unify Enterprise takes a modular approach, giving you the functionality to administer only AD out of the box. If you need to provision Exchange Server or another "external" system, you'll need to purchase additional components. Unify Enterprise can be extended to support BlackBerry Enterprise Server, Exchange 2007 or 2003, Google Apps, and Microsoft Office Communication Server (OCS).

ManageEngine ADManager Plus

The Manage Engine website immediately draws your attention to the company's *90:10 Promise*: "90 percent of the features of the Big 4 at 10 percent of the price." I wondered whether the product could really deliver on that promise. After testing, I wasn't so sure.

I downloaded the 30MB installation file and started the setup process. This was by far the easiest and fastest installation of all of the four products. I needed only to specify the port that I wanted the web server to run on (the default is port 8080).

ADManager Plus has the most comprehensive list of available reports.

As with the other products, the main GUI is web-based. However, ADManager can be authenticated with either domain or ADManager Plus authentication. Once you're logged on, a dashboard of canned reports shows you the number of active users, inactive users, disables users, locked out user, and so on. Figure 2 shows additional details. The tabs available across the top are AD Mgmt, AD Reports, AD Delegation, Admin, and Support.

ADManager Plus has a clean layout for adding or modifying user and computer accounts. You can move users one at a time or in bulk through a CSV import. A feature that sets this product apart from the competition is its Bulk User Modification. For example, you can move the Home Folders, disable/enable accounts, or change the dial-in/VPN properties for a group of users. You can also alter Exchange and Terminal Services attributes.

There are multiple built-in roles that can accomplish the most common tasks, such as creating users, resetting passwords, and unlocking users. Alternatively, you can create custom roles with specific rights that can perform custom tasks. I was excited to see a particular right: Create Exchange Mailbox. With this right, I was able to create a Help Desk Technician Role that had the correct permissions to create an Exchange mailbox, even though the user wasn't an Exchange administrator.

ADManager Plus has limited capability for provisioning Exchange above and beyond what you get with the standard Microsoft tools. Whereas some of the other applications can automate the Exchange portion, ADManager can't. Because ADManager Plus can't provision outside AD or Exchange, I focused my testing on disabling and deleting accounts. A Delete policy lets you specify whether a user's Home Folder, Roaming Profile, Terminal Server Home Folder, or Terminal Server Profile should be deleted along with the user account. One important note: I couldn't find a "recycle bin" feature. When an AD object is deleted, it's deleted just as if you removed the object through the built-in Microsoft Management Console (MMC) Active Directory Users and Computers snap-in.

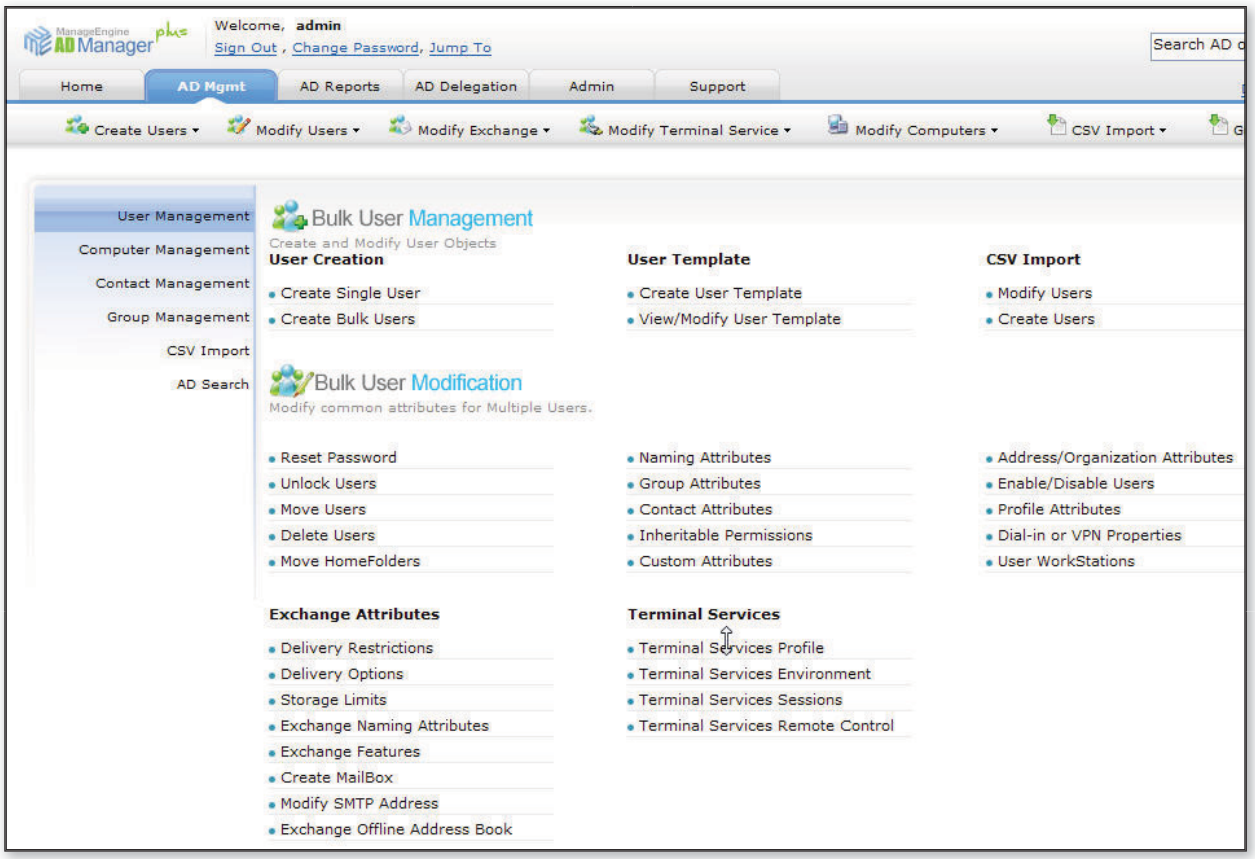


Figure 2: ManageEngine ADManager Plus

ADManager Plus includes 13 types of reports, including password, Exchange, GPO, OU, and many others. There are even compliance-specific reports, including SOX-, HIPPA-, and PCI-compliance reports. Of all the products in this comparative review, ADManager Plus has the most comprehensive list of available reports.

NetIQ Directory and Resource Administrator

NetIQ Directory and Resource Administrator has both a web interface for day-to-day administrative tasks, as you see in Figure 3, page 72, and separate applications for *Account and Resource Management* and *Delegation and Configuration*. Like the other products in this review, NetIQ Directory and Resource Administrator is considered a 100 percent proxy model. In other words, "real" AD permissions aren't actually granted to your junior administrators. This is a real advantage if the OU structure of your AD implementation wasn't set up correctly correctly—particularly if the objects you want to grant access to aren't grouped in your OU structure.

This product promotes the notion of *powers*, which are similar to rights. There are 290 preconfigured powers, and you can also create your own. A simple wizard lets you create a new power over users, groups, computers, contacts, OUs, and published printers. For example, I created a power that allowed the user property EmailAddress to be updated. These powers are then combined to create roles (e.g., Help Desk Administrator). The product's administration website is great for non-technical users, such as managers who have the *reset password* power, or even for users who have permission to update their personal information (e.g., job title, phone numbers).

Another concept unique to NetIQ Directory and Resource Administrator is *automation triggers*. A new trigger is created and associated with a UserCreate operation. Once this has been set up in the product's Delegation and Configuration tool, an administrator or Help desk technician can use the web interface to create users, configure Exchange mailboxes, and so on. The interface is simple and well designed.

You can also perform Exchange provisioning through the Delegation and Configuration tool. A simple checkbox enables Exchange 2007, 2003, and/or 2000 support. Although this out-of-the-box feature set is pretty basic, NetIQ provides a free Knowledge Script Depot to all its customers. A quick search of the scripts resulted in a script called CreateMailbox_on_Specific_Store.vbs.

With the product's ActiveViews, you can implement delegated authority independent of your AD structure. This is useful if the current OU structure wasn't set up properly or if the areas you want to delegate control of fall outside the scope of your current OU structure. An ActiveView can be a group of just about anything, including users, groups, OUs, contacts, computers, and even resources such as printers, print jobs, shares, and services. Because ActiveViews are dynamic (much like an Exchange query-based distribution list), these views change and grow as your domain changes, with no administrative overhead on your part. I was able to easily create an ActiveView that included all

Ensim Unify Enterprise Edition

PROS: Simple, easy-to-navigate interface; built-in roles help get you started

CONS: No ability to export reports for easy access by an auditor

RATING: ◆◆◆◇◇

PRICE: Starts at $12 per user

RECOMMENDATION: If you need provisioning outside AD, look no further.

CONTACT: Ensim • 877-693-6746 • 408-496-3700 • www.ensim.com

ManageEngine ADManager Plus

PROS: Perfect UI; extremely easy to navigate

CONS: No user provisioning outside of AD and Exchange

RATING: ◆◆◆◇◇

PRICE: $1,495 for the Professional edition

RECOMMENDATION: ADManager Plus gets my recommendation as an inexpensive alternative to Active Directory Users and Computers; it provides more features than the built-in snap-in.

CONTACT: ManageEngine • 888-720-9500 • 925-924-9500 • www.manageengine.com

NetIQ Directory and Resource Administrator

PROS: Outstanding auditing and reporting capabilities; simple and well designed interface

CONS: Heavy use of scripting required to automate external apps; not as intuitive as ActiveRoles Server

RATING: ◆◆◆◆◇

PRICE: $1,600 for 100 users

RECOMMENDATION: If you need superior auditing and reporting, and you're comfortable using VBScript for external automation, this product comes highly recommended.

CONTACT: NetIQ • 888-323-6768 • www.netiq.com

Quest Software ActiveRoles Server

PROS: Extremely robust AD user-provisioning tool

CONS: Expensive

RATING: ◆◆◆◆◇

PRICE: $25 per AD user; additional costs for external connections

RECOMMENDATION: If you need full user provisioning with detailed workflow functionality, Quest ActiveRoles is your best choice

CONTACT: Quest Software • 800-306-9329 • www.quest.com

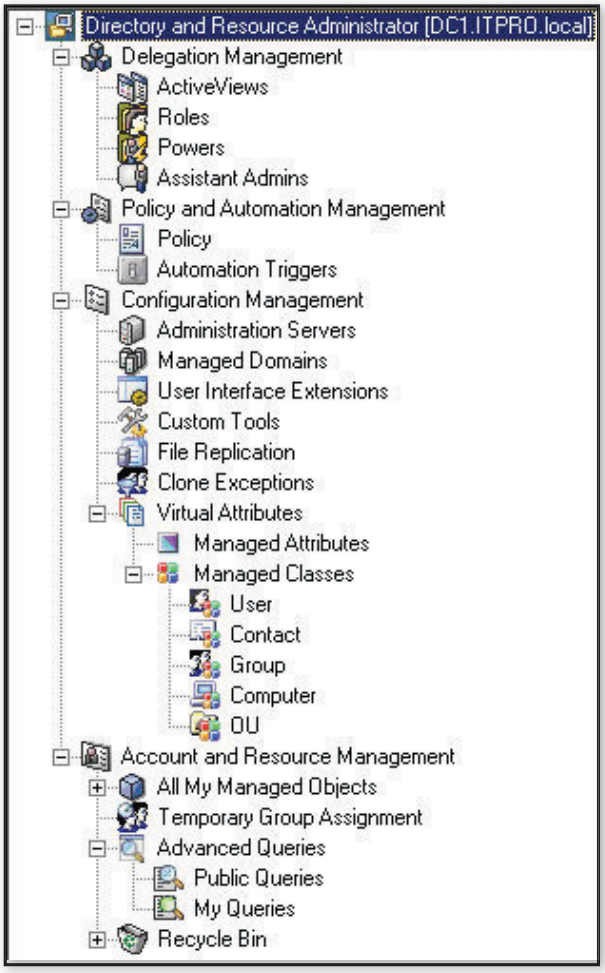


Figure 3: NetIQ Directory and Resource Administrator

the users from the Spokane, WA office. After you create an ActiveView, another wizard automatically starts, letting you delegate specific control of that view to a group.

To generate a report on any object in AD, you use the Directory and Resource Administrator (not the web interface). This tool lets you query for a specific user or group (or any object) and run a report of changes made to (or by) the object. For example, you might want to know who has altered the Help Desk Administrators group (has someone added a rogue entry?), or you might want to know what this particular group has been doing. I found the reporting to be very granular and detailed enough to make any auditor happy.

Provisioning a new user in ActiveRoles Server was easily the most user-friendly process of all four products.

Quest Software ActiveRoles Server

If you've ever used the built-in Delegate Control feature in the Active Directory Users and Computers snap-in, you'll feel right at home in ActiveRoles Server, which Figure 4 shows. The product has three default web components: Self Service, Help Desk, and Administrators.

Provisioning a new user in ActiveRoles Server was easily the most user-friendly process of all four products. The built-in policies do a great job of getting you most of the way there. And like the other products, this one requires that you go the rest of the way with scripting. If you're unsure where to begin, Quest has a handy Wiki document full of useful scripts that you can plug directly into ActiveRoles Server.

At one company I've worked with, Help desk technicians aren't allowed to create Exchange mailboxes because of the "risk that they might not create the mailbox in the correct store." This scenario frustrates the junior technician and wastes the senior engineer's time. ActiveRoles Server's provisioning and de-provisioning policies help in these kinds of situations.

When a user leaves the company, ActiveRoles Server can take care of the Exchange portion of the task as well, hiding the mailbox from the Global Address List (GAL), granting the user's manager full access to the user's mailbox, and forwarding all new incoming messages to the manager.

VirtualizationPro

2010 SUMMIT & EXPO

MARCH 16-19, 2010
BELLAGIO—LAS VEGAS, NV
www.VirtualizationProSummit.com

CONNECT WITH INDUSTRY EXPERTS!

Steve Riley | Michael Otey | Dan Holme | John Savill | Alan Sugano

www.VirtualizationProSummit.com
800-438-6720 or 203-400-6121

Windows IT Pro | SQL Server magazine | TECH Conferences Inc. | PENTON MEDIA | PENTON

VirtualizationPro
2010 SUMMIT & EXPO

MARCH 16-19, 2010
BELLAGIO—LAS VEGAS, NV
www.VirtualizationProSummit.com

Top 10 Reasons to Attend the Virtualization Pro Summit

10. Learn how to take virtualization technology to the next level for the benefit of your organization.
9. Find out from industry insiders the best virtualization technologies.
8. Learn the differences between Microsoft Hyper-V and VMware ESX Server.
7. Choose from over 24 sessions delivered by industry experts.
6. Enroll to attend the VirtualizationPro Summit sessions and you can also attend any of the co-located SharePointPro Summit sessions for FREE!
5. Attend sessions on current technology as well as highlights of the new stuff.
4. Extend your professional and social network at our events outside of the sessions.
3. Find products and services from our partners in the Expo Hall that can save money, save time, and help your business do more.
2. Book your hotel early and take advantage of GREAT hotel rates at Bellagio Hotel & Casino. Enjoy a 4-star experience at a 2-star price on the Las Vegas Strip!
1. Enjoy the excitement and luxury of one of Las Vegas' premiere hotels while you experience one of the best technical conferences of your career. You know that Las Vegas is famous for some of the best dining, shows, shopping, and 24/7 buzz of anywhere in the world.

SCHEDULE at a glance

TUESDAY, MARCH 16, 2010	
7:30 am - 5:00 pm	Conference Registration
9:00 am - 4:00 pm	Pre-conference Workshops
6:30 pm - 8:30 pm	Opening Keynote
8:00 pm - 10:00 pm	Expo Hall Open
WEDNESDAY, MARCH 17, 2010	
7:30 am - 5:00 pm	Conference Registration
7:30 am - 8:30 am	Continental Breakfast
8:30 am - 11:30 am	Conference Sessions
11:30 am - 1:00 pm	Lunch
1:00 pm - 4:00 pm	Conference Sessions
8:30 am - 5:00 pm	Expo Hall Open
5:00 pm - 6:30 pm	Expo Hall Giveaways
THURSDAY, MARCH 18, 2010	
7:30 am - 5:00 pm	Conference Registration
7:30 am - 8:30 am	Continental Breakfast
8:30 am - 11:30 am	Conference Sessions
11:30 am - 1:00 pm	Lunch
1:00 pm - 4:00 pm	Conference Sessions
8:30 am - 4:00 pm	Expo Hall Open
FRIDAY, MARCH 19, 2010	
7:30 am - 8:30 am	Continental Breakfast
8:30 am - 11:30 am	Conference Sessions

Sean Deuby

Sean Deuby, a Senior Enterprise Solutions Strategist with Advaiya, Inc., has 25 years' experience in enterprise IT. He spent over a decade running Texas Instruments' IBM VM systems — the first virtualized operating system — then designed, deployed, and supported TI's first Windows NT 3.5 worldwide infrastructure. He also spent 10 years with Intel Corporation, where he was the design engineer of the core directory services team and one of the architects of Intel's corporate Active Directory forest. Sean has been a Contributing Editor for *Windows IT Pro* magazine for 10 years. Sean is a regular and highly rated speaker at Tech Ed and Windows Connections conferences.

Wendy Henry

Wendy Henry is a Microsoft Certified Trainer (MCT) who has been an independent technical trainer, author, and consultant for more than 10 years. She has specialized in Microsoft SQL Server since 1999 and SharePoint since 2005. Wendy is a contributing partner on SharePoint-eLearning.com and frequently teaches and presents at conferences on WSSv3/MOSS2007.

Dan Holme

A graduate of Yale University and Thunderbird, Dan has spent 15 years as a consultant and trainer, delivering solutions to tens of thousands of IT professionals from the most prestigious organizations and corporations around the world. Dan's company, Intelliem, offers deep expertise and experience in Windows, Active Directory, and SharePoint. From his base in beautiful Maui, Dan travels around the globe supporting customers and delivering Microsoft technologies training. Dan is also a contributing editor for *Windows IT Pro* magazine and a Microsoft MVP (Windows Server Directory Services, 2007, and Office SharePoint Server, 2008-2009). Dan is currently building SharePoint solutions to support the broadcast of the 2010 winter Olympics in Vancouver as the Microsoft Technologies Consultant for NBC Olympics.

Satish Jakka

Satish Jakka, Managing Editor at Platform Vision, has more than 15 years of experience. Before joining Platform Vision, he spent close to 10 years at Microsoft, where he worked as an Infrastructure Architect. Prior to that, Satish worked as a Senior Program Manager in the MSDN and TechNet product groups. Before Microsoft, Satish was Team Lead, Information Systems and Services for UUNET.

Heath Madison

Heath Madison, Director of Core Infrastructure at Advaiya, Inc., has been working in information technology since 1993 and specializes in Microsoft solutions. He has also served as a senior consultant and architect for implementing technology in global corporations. Heath has a thorough knowledge of Microsoft systems and solutions in addition to many third-party hardware and software tools.

Michael Noel

Michael Noel is an MVP for SharePoint Server and an MCSE+I. He has been involved in the computer industry for nearly two decades, and has significant real-world experience helping organizations realize business value from Information Technology. Michael has authored several major best-selling industry books that have been translated into seven languages with a total worldwide circulation of over 150,000 copies. Currently a partner at Convergent Computing in the San Francisco Bay Area, Michael's writings and worldwide public speaking experience leverage his real-world expertise designing, deploying, and administering IT infrastructure for his clients.

Michael Otey

Michael Otey, technical director for *Windows IT Pro* and *SQL Server Magazine*, is president of TECA, a software-development and consulting company in Portland, Oregon, and coauthor of SQL Server 2005 Developer's Guide (Osborne/McGraw-Hill). Michael has covered the topic of virtualization extensively for *Windows IT Pro* magazine, having written several features articles showing how to take advantage of virtualization in the enterprise as well as reviewing all of the major virtualization products.

Steve Riley

Steve Riley is an evangelist and strategist for cloud computing at Amazon Web Services, working to help organizations understand how to integrate their environments with the cloud to extend reach, increase utilization, and respond to rapid business changes. His specialties include information security, compliance, reliability, privacy, and policy. Steve is a popular speaker at conferences worldwide, meets regularly with user groups of all sizes, and seeks opportunities to engage with customers as often as possible.

John Savill

John Savill , Manager, Solutions Architecture at EMC, is a nine-time Microsoft MVP, and is recognized worldwide for his superior product knowledge and practical skills. He is the author of Windows Server 2003 Active Directory Design and Implementation, The Windows XP/2000 Answer Book, and The Windows NT and Windows 2000 Answer Book, and contributor to several Windows-related books in the "For Dummies" series of reference books. In addition, he serves as a contributing editor to various publications on Microsoft products including *Windows IT Pro* and *SQL Server Magazine*.

Alan Sugano

Alan Sugano is the president of ADS Consulting Group, Inc. (ADS), which specializes in networking, custom programming, Web development, SQL Server development, and ACCPAC Plus accounting implementations. Alan frequently delivers talks on network audits, server selection, network documentation, network management, network design and topologies, SQL Server databases, and disaster recovery.

PRE-CONFERENCE SESSIONS

Half-Day: (9am-noon) Virtual Desktop Infrastructure—Is It Really Something You Want or Need?

In this session we look at what VDI really entails, the architectural options we have for our design and the components needed. We will examine environments where VDI works well and how an organization goes about performing the business justification to really make sure VDI is something that they should be doing. Microsoft, VMware and Citrix technologies will be examined as possible solution points and how they can play well together.

Half-Day: (1pm-4pm) Implementing App-V

JOHN SAVILL

Virtualization is everywhere with Virtual Desktop Infrastructure gaining momentum in many environments. But one key technology is often overlooked and not fully understood: the virtualization of the applications. Formally known as SoftGrid, App-V is Microsoft's application virtualization solution. App-V allows the local execution of applications on an operating system without installing the application. The virtualization of applications solves two critical problems, application-to-application incompatibility and instant application launch for first-time use, which is crucial in any VDI scenario. In this session we'll look at the underlying architecture of App-V, how exactly App-V functions and solves the mentioned application challenges, and best practices around App-V architecture and deployment through a live implementation of an App-V environment. At the end of the session attendees will have a strong understanding of how App-V works, when and when it shouldn't be used, and how to get App-V deployed in their environment.

Full Day: (9am-4pm) Technical Face-Off: Hyper-V and ESX

DEAN DEUBY, SATISH JAKKA, HEATH MADISON

If you're still trying to decide whether to implement Vmware's vSphere 4.0 or Microsoft's Windows Server 2008 R2 Hyper-V based virtualization solution, here's your chance to get the straight dope. Experts Sean Deuby, Satish Jakka, and Heath Madison of Platform Vision bring their Faceoff blog and poster (http://windowsitpro.com/faceoff) to life in this day-long session. Using examples and demonstrations, they will take an unbiased look at the two hypervisors and their management solutions, with the goal of helping you determine which issues are really important to you—and which are just hype. Topics will include the different hypervisor configurations, memory management, licensing, security, patch management, and the strengths and weaknesses of recommended management solutions from each vendor. This is a unique opportunity to learn from unbiased experts about the differences between each vendor's server virtualization solution so that you can make your own decisions based on side-by-side platform comparisons.

Keynote:
Stepping Into the Cloud

STEVE RILEY

Virtualization is one of the many key components of cloud computing. Indeed, without mature virtualization technologies and practices, cloud computing wouldn't be what it is today. And it's here to stay: unlike the application service provider days of the late 1990s, cloud computing is already changing the way many organizations store, process, and distribute information. Yet many other IT shops remain wary. Moving compute and storage out of your own data center and into someone else's, mingled among many others, seems daunting at first. Common questions arise around security, manageability, performance, and reliability. Think about it, though—these are the same concerns you've always had. Nothing about the cloud requires that you jettison everything you've learned during your career. The cloud is a logical next step in the evolution of computing, and when integrated with corporate IT removes much of the burden and allows a business to concentrate on its core functions. Steve Riley will introduce typical cloud architectures, explore common concerns, dispel several myths, discuss how to "think cloud," and help you learn how your business can benefit from the cloud.

BREAKOUT SESSIONS:

Virtualization and Security

STEVE RILEY

Securing an environment composed of virtual servers and clients presents certain distinct challenges, but it doesn't require you to throw away everything you already know. Virtualization follows a noticeable trend in the evolution of computing technologies; being aware of this helps us understand how to ensure that virtualized environments aren't suddenly vulnerable to attacks. Virtualization makes certain security-related tasks easier and more cost-effective, like application testing and deploying honeypots. Securing virtualized resources builds on the experience you already have and requires a few additional things to consider. Steve Riley will explore these topics and also examine security technologies deployed by Amazon Web Services in its implemention of the Xen hypervisor used in Amazon's Elastic Compute Cloud.

Highly Available Virtual Infrastructures

JOHN SAVILL

This session will explore technologies to help with planned and unplanned host downtime with both Hyper-V and VMware—and the pros and cons with the technologies used. We will also explore features related to storage and network migration without impacting guest instances.

Live Migration Step-by-Step

MICHAEL OTEY

In this session you'll learn about Hyper-V 2.0's Live Migration capability. You'll learn about requisites that need to be in place to

use Live Migration—and you'll follow along on a step-by-step guide to configuring and using Live Migration.

Virtualization of Exchange Server 2010 Architecture

MICHAEL NOEL

The advantages of server virtualization are significant and many organizations have been making the move toward virtualization of core components in their infrastructure, including Exchange Server. Virtualizing Exchange Server has certain significant challenges, however, and it is important to understand how to properly scale a virtualization environment to handle the unique requirements of Exchange. The latest version of Exchange Server provides for key virtualization advantages such as lowered Disk IO, multiple database copies using Database Access Groups (DAGs), and other enhancements that change the virtualization design paradigm. This session focuses on real-world best practice architectural guidance for virtualizing an Exchange Server environment, with particular focus on Exchange Server 2010 server roles and architecture. Real-world virtualized Exchange Server 2010 designs and deployments of varying sizes are discussed and compared.

- Understand how and when to virtualize Exchange Server 2010 server roles and components
- Determine the best virtualized Exchange Server architecture for your environment
- Learn the caveats, risks, and challenges that may be encountered in a virtualized Exchange environment

Server Virtualization Basics

ALAN SUGANO

As server hardware becomes more powerful, much of the processing power of the server is wasted. Server Virtualization allows you to efficiently use the processing power of new servers and the 64-bit platform by consolidating multiple physical servers onto a single virtual server host. We'll look at virtualization software technologies and how they work with server virtualization. We'll examine hardware configuration issues in the virtualization environment and offer tips on selecting the proper hardware for server consolidation. We'll review consolidation strategies to ensure that no one virtual server host is overloaded with virtual server guests. Virtualization has the potential to save money, reduce server setup time, provide a flexible test environment, speed up disaster recovery, and still provide high availability.

How Many Virtual Machines Can I Cram on This Box?

JOHN SAVILL

In this session, we'll examine the technologies that help achieve high virtual machine densities on your virtual infrastructure. We'll look at features that enable memory, CPU, and disk sharing between virtual machines and how Hyper-V and VMware can help consolidate on as few virtual servers as possible without impacting guest performance.

Designing Virtualized Storage for Resilience

Do you know where your VM data is? T-Mobile thought it did, right up to the point where all Sidekick users in the U.S. found their contacts and calendars missing. VM technology concentrates risk, which means you must design back-end SANs appropriately to mitigate those risks. Learn how to measure and counter vulnerabilities that arise out of having your eggs in an insufficient number of baskets.

ESX vs. Hyper-V

MICHAEL OTEY

Learn the differences between Hyper-V 2.0 to ESX Server 4.0 as Michael explores the architecture of the two products and compares their overall feature sets. You'll get an overall feature comparison as well as a cost comparison. You'll also learn about

the types of businesses each product is best suited for.

PowerShell Management for Virtualization: Hyper-V

SATISH JAKKA

Come learn how to use PowerShell to automate deployment and management of your virtualized infrastructure. See how you can leverage PowerShell across the Microsoft virtualization platform and go beyond to see PowerShell manage your applications through the entire application lifecycle.

Managing the User Experience across Physical and Virtual Environments

DAN HOLME

As enterprises turn to virtualization, in all its forms, users begin to "roam" in ways we never imagined just a few years ago. Even if a user sits at a single physical device, their experience stretches across remote desktop sessions, virtual machines, and virtualized applications. In order to maintain, let alone improve, productivity you must ensure a consistent, manageable and supportable workspace for your users. The pieces are all there: folder redirection, user profiles, group policy, ACLs, encryption, and DFS. But the intricacies and interactions of these technologies are surprisingly complex, and until you start managing them, your IT service delivery will suffer. In this session, you will learn best practices for putting the pieces together. Participants are expected to have a solid understanding of most or all of these technologies or be ready to learn them offline. This advanced session prepares you to take away ready-to-implement, useful solutions to corralling, securing, and managing user data and settings in both physical and virtual environments.

Virtualization's Role in Disaster Recovery

ALAN SUGANO

A comprehensive Disaster Recovery Plan is something that every company should have and hopefully will never have to use. Having a plan in place that provided a road map to recovery was adequate in the past, but recent emphasis has been placed on the speed of the recovery. Sarbanes-Oxley (SOX) compliance companies must disclose their business continuity plans and the company's exposure to a prolonged outage and how it affects financial reporting. Virtualization can significantly reduce the recovery time for a major disaster, by providing a warm or hot remote recovery site and accelerating workstation and server setup.

Understanding Virtualization Technologies

MICHAEL OTEY

Virtualization encompasses a virtual maze of technologies. Let Michael lead you through the maze as he explains the different types of virtualization. You'll learn about the difference in desktop and server virtualization as well as application virtualization. You'll also see where each of today's popular products fits in.

Virtualizing Your Active Directory Forest

SEAN DEUBY

Virtualization is all the rage today. Can you apply virtualization to the critical infrastructure of your Active Directory forest? When does

it make sense, and when should you leave it alone? Learn how to safely virtualize your domain controllers, understand security and recovery concerns, and apply virtualization to cheaply enable advanced domain recovery capabilities.

VMware: Performance Tuning and Configuration

SATISH JAKKA

Learn the art of tuning your VMware infrastructure for performance. In this session we will discuss the relationship between server workloads and CPU cores, memory, and storage. We will also discuss configuration, optimization and monitoring of workloads.

Automating the Dynamic Datacenter and Creating Virtual Machines Automatically

JOHN SAVILL

One of the key benefits of virtualizing the environment is a streamlined and accelerated provisioning process for operating system instances. In this session, we'll look at what a dynamic datacenter really is and the methods and technologies we can and should be using for the creation of virtual machines in our datacenter. We'll examine solutions from Microsoft and VMware. And in addition to just creating our virtual environment, we'll see how to maintain the datacenter most efficiently and how to automate provisioning of virtual environments for end users.

Has Virtualization Decreased the Importance of SQL Server Backups?

WENDY HENRY

So, how long does your hardware take to perform a full backup and restore of your largest SQL Server database? As virtualization platforms have matured, so have the underlying storage facilities smart networks employ to reap the hardware utilization and ROI benefits of virtual machines without suffering performance degradation. Many virtualization and storage platforms offer advanced snapshot and availability features that you can use to redirect users to previous versions of mission-critical data without the delays of traditional restore operations. Have these features eliminated the need for traditional backup and restore disaster recovery strategies? In this session, we'll explore the idea of using virtual versioning and archiving in place of traditional SQL Server database backups to satisfy the immediate access demands of today's business users.

A Compelling Look at vSphere 4.0

ALAN SUGANO

vSphere 4.0 is VMware's next release of their Hypervisor. It represents VMware's move from a 32-bit Hypervisor in ESX 3.5 to a 64-bit Hypervisor in vSphere 4.0. The performance improvement, especially in CPU-intensive applications, is significant. In fact, you could justify the upgrade based on the improved performance alone. Besides the performance aspects there are a significant number of new features in vSphere, Some including

1. vSphere Bundles
2. 64-bit Hypervisor
3. Host Profiles
4. VMKernel Protection
5. Improvements in Fault Tolerance
6. VMotion Enhancements
7. vShield Zones
8. Hot Add Support
9. Power Management
10. Thin Provisioning
11. Fibre Channel over Ethernet (FCoE) Support
12. vNetwork Distributed Switch

Learn about these new features and how they can benefit your company's virtualization IT strategy.

Distributed File System: The Cheapskate's Storage Virtualization

SEAN DEUBY

Microsoft's Distributed File System provides a way to easily separate how your users access their data from where the data's located on your network. And it needn't cost you anything to implement it! Learn how to use it to quickly and easily build, manage, and delegate an easy to use enterprise virtual folder structure.

PowerShell Management for Virtualization: VMware

SATISH JAKKA

Come learn how to use PowerShell to automate deployment and management of

your virtualized infrastructure. See how you can leverage PowerShell across the VMware virtualization platform and go beyond to see PowerShell manage your applications through the entire application lifecycle.

vSphere vs. System Center

MICHAEL OTEY

Come to this session to learn how vSphere compares with Microsoft's System Center. You'll get an overall feature comparison as well as see how each product addresses different management concerns in the organization.

Application Virtualization

ALAN SUGANO

End the patch management hell. Application virtualization allows you to run applications without having to install the application on each workstation. This simplifies patch management and significantly reduces the time to roll out new or upgraded applications, because patches are installed once on the application server and not individually on each workstation. We'll take a look at Microsoft's Softricity technology and how it handles local, remote, and disconnected clients and their applications. This technology also leads to the software as a service directive that many companies see as an industry trend. Application virtualization also ties into disaster recovery because it significantly reduces the prep time for workstation recovery. Application virtualization can reduce patch management headaches, reduce the time to roll out new applications, easily roll back problematic patches, allow users to run different versions of the same application, and speed up disaster recovery. See if this technology is a good fit for your company.

System Center Virtual Machine Manager: Real Control for Your Virtual Environment

SEAN DEUBY

Managing your Microsoft or VMware virtual machines presents a different set of challenges than managing physical servers. Virtual systems move around on different physical hosts, they can be quickly provisioned or de-provisioned, their large disk images present unique management, security, and performance challenges…the list goes on. Microsoft's System Center Virtual Machine Manager (SCVMM) is designed to handle all these challenges of managing virtual systems from both Microsoft and VMware, from workgroup-sized configurations to full enterprise deployments. Check out this session to learn how to quickly begin using SCVMM to manage your virtual environment.

Virtualization of SharePoint 2010 Farm Architecture

MICHAEL NOEL

Server virtualization technologies have taken center stage recently and many organizations have begun to replace physical servers, including SharePoint servers, with virtualized machines. Virtualization of the 2007 wave of SharePoint Products and Technologies has been supported for some time, and many 2007 farms have been successfully virtualized over the years. With a new version of SharePoint, however, comes new best practices and new techniques for virtualization of SharePoint. This session focuses specifically on SharePoint Server 2010 farm virtualization and how components of a SharePoint 2010 environment can be successfully virtualized. Included in the discussion are new virtualization high availability options such as Windows Server 2008 R2 Hyper-V Live Migration of SharePoint guest sessions as well as time-tested design architecture examples using integrated SharePoint failover techniques.

- Learn the best practices for virtualizing the new architectural elements of a SharePoint 2010 farm
- Examine real world designs of virtualized SharePoint farms of varying sizes and functions
- Understand how to properly size a SharePoint environment by reviewing real world sizing guidelines for virtual hosts, guests, server and storage infrastructure

VirtualizationPro 2010 SUMMIT & EXPO

RESERVE YOUR ROOM EARLY to take advantage of great hotel discounts!

HOTEL ACCOMMODATIONS

Bellagio Las Vegas
3600 Las Vegas Blvd South
Las Vegas, NV 89109

Bellagio Las Vegas is the conference site and host hotel. This is where all sessions and activities are held. Hotel requires a one night's deposit at time of reservation. (Credit card will be charged by the hotel). Hotel cancellation policy: Must cancel at least 72 hours prior to arrival date.

The special conference rate will be honored starting two days before the start of conference through two days after the end of the conference, based upon availability. Space is limited so reserve your room early by registering online or by calling the conference hotline at 800-438-6720 or 203-400-6121. All reservations must be guaranteed with a major credit card to confirm room. A deposit of the first night room and tax will be charged. Cancellations must be received by the hotel 72 hours prior to the confirmed arrival date to receive refund of deposit.

TRANSPORTATION

Taxis are available right outside of the baggage claim area of McCarran International Airport. Taxi Ride will average approximately $18.00 (subject to change) to the Bellagio Las Vegas.

ATTIRE

Conference dress is comfortable and casual. Temperatures in Las Vegas are about 68° F (20°C) in March. The session rooms are air conditioned so you may want to bring a sweater.

TAX DEDUCTION

Your attendance to the VirtualizationPro 2010 Summit & Expo may betax deductible. Visit www.irs.ustreas.gov. Look for topic 513 - Educational Expenses. You may be able to deduct the conference fee if you undertake to (1) maintain or improve skills required in your present job; (2) fulfill an employment condition mandated by your employer to keep your salary, status, or job.

GROUP DISCOUNT

Register individuals from one company at the same time and receive a group discount.

1-3 registrants: $1,395 per person

Additional registrants after the 3rd: $1,195 per person ($200 off each)

Call 800-438-6720 to take advantage of group discount pricing.

NOTES & POLICIES

The Conference Producers reserve the right to cancel the conference by refunding the registration fee. Producers can substitute speakers and topics and cancel sessions without notice or obligation. Updates will be posted on our Web site at www.VirtualizationProSummit.com. Tape recording, photography is not allowed at any session. Conference producers will be taking candid pictures of events and reserve the right to reproduce. By attending this conference you agree to this policy. You may transfer this registration to a colleague by notifying us before the start of the event. Please inform us if you have any special needs or dietary restrictions when you register. The conference registration includes the following subscription. This is not an additional expense and subtraction from prices listed is not permissible. VirtualizationPro 2010 Summit & Expo registration includes a one year (12 issues) print subscription to Windows IT Pro magazine. Current subscribers will have an additional 12-months added to their subscription. Subscriptions outside of the United States and Canada will be served in digital; $12.50 of the funds will be allocated toward a subscription to Windows IT Pro magazine ($49.95 value).

Registration & Cancellation Policy: Payment must be received before the start of the conference. Cancellations by February 15th, 2010 must be received in writing and will be refunded minus a $100 processing fee. After February 15th, 2010 cancellations and no-shows are liable for full registration fee, however registration can be transferred to the next Conference within 12 months or to another person.

CONFERENCE REGISTRATION

ONLINE
www.virtualizationprosummit.com

PHONE
800.438.6720
203.400.6121

FAX
913.514.9362

MAIL
VirtualizationPro Summit & Expo
c/o Tech Conferences, Inc.
731 Main Street, Suite C-3
Monroe, CT 06468

Name | Priority code

Company | Title

Street Address (Required to ship materials)

City, State, Postal Code | Country

Telephone | Fax | E-mail Address (important)

VIRTUALIZATIONPRO 2010 SUMMIT & EXPO	PRICE	SUBTOTAL
on or before January 15, 2010	$1195.00	
after January 15, 2010	$1395.00	
Early Bird Bonus: Register for the conference and hotel (on or before January 15th) and receive a $100 Bellagio Gift Card. (3 night minimum stay at host hotel required)		

PRE-CONFERENCE WORKSHOPS | Tuesday, March 16,2010 | Lunch is included with full day workshops			
Half-Day (9 AM - 12 PM)	Virtual Desktop Infrastructure --Is It Really Something You Want or Need?	$199.00	
Half-Day (1 PM - 4 PM)	Implementing App-V—John Savill	$199.00	
Full Day (9 AM - 4 PM)	Deep Dive Comparison of Hyper-V and ESX—Sean Deuby and Satish Jakka	$399.00	

PAYMENT

TOTAL

*IMPORTANT: You must reference VirtualizationPro Summit & Expo on your check.

☐ CHECK (payable to Tech Conferences) All payments must be in US currency. Checks must be drawn on a US bank.

☐ VISA ☐ MASTERCARD ☐ AMEX

Cardholder's Signature | Cardholder's Name (rint)

VirtualizationPro
Summit & Expo
c/o Tech Conferences, Inc.
731 Main Street, Suite C-3
Monroe, CT 0648

Mailroom: If addressee is no longer here,
please route to MIS Manager or Training Director

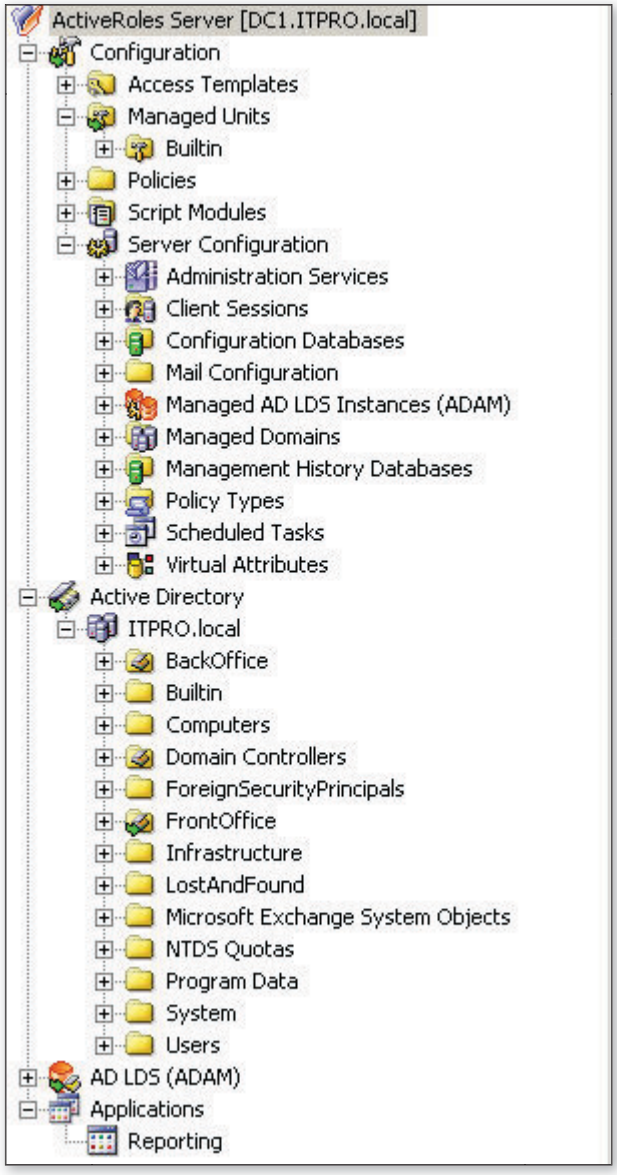


Figure 4: Quest ActiveRoles Server

This tool looks and feels the most like AD itself. When you're delegating permissions, you'll find that the ActiveRoles delegation wizard looks and feels almost identical to Active Directory Users and Computers. Also, whereas ActiveRoles is a "proxy" type tool by default (e.g., ActiveRoles Server controls the permissions, not AD), you can sync the permissions that you set up to AD if you want to. This functionality is useful if applications outside ActiveRoles Server—such as an HR database—need to access objects in AD.

Similar to NetIQ with its ActiveViews, ActiveRoles Server has a feature called Managed Units (MUs). An MU is a collection of objects that you want to group together for administration. As in the NetIQ example, this is useful if the domain wasn't designed properly or even if the administrative tasks you want to perform are outside the AD design. For example, your OU structure might be by city or department, with individual managers distributed throughout the structure. An MU could include all the managers in a particular city and then be granted the right to reset passwords.

ActiveRoles Server has robust Exchange provisioning capabilities, including user and group de-provisioning. When de-provisioning a user, you can disable the account, set the username and password to random values, remove the account from security or distribution groups, grant the manager permissions to the user's home folder, delete the home folder, run a script (PowerShell, VBScript, JScript, or PerlScript) to delete the employee from an HR database, and schedule the account for permanent deletion.

Before the ActiveRoles Server system can be used for reporting, a Data Collector has to be installed on the server first. Another SQL Server database also has to be created to store the data. The process for getting reporting set up in this product was the most complex of all these products. In fact, throughout testing, I couldn't get the reporting to work correctly.

Editor's Choice

These products are heads and shoulders above the AD tools that Microsoft ships with Windows Server. However, don't consider them substitutes for proper planning and management! More than once, I found that if I was careless (or sneaky) enough, I could find a way for a Help desk technician to escalate his or her privileges and get added to the Domain Administrators group. This isn't a fault of the tools, but they can make it easier to become complacent.

Each of these products worked well and performed its tasks as advertised, but in my opinion, ActiveRoles Server edges out the competition. I appreciate that even though it has a "proxy" model like the other products, the permissions can also be synced to the native AD security structure. The built-in policies to provision and de-provision users immediately subtracts about 30 minutes of busy-work in the typical IT shop when a user is terminated. ActiveRoles Server also has a robust, built-in Workflow module. In the end, ActiveRoles Server simply impressed me the most, regardless of the trouble I experienced with the reporting feature. NetIQ Directory and Resource Administrator ranks a close second, only because ActiveRoles Server has a stronger interface.

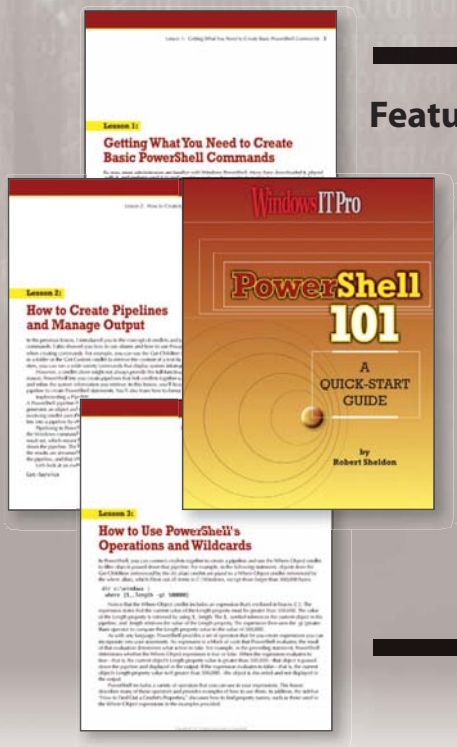
InstantDoc ID 103318

ERIC B. RUX
(ebrux@whshelp.com) is a contributing editor for *Windows IT Pro* and cofounder of WHSHelp.com. He writes a column at svconline.com/connectedhome and teaches the Microsoft Certified Systems Administrator (MCSA) program at a tech college.

Prime Your Mind

with Resources from Left-Brain.com

Left-Brain.com is the newly launched online superstore stocked with educational, training, and career-development materials focused on meeting the needs of IT professionals like you.



Featured Product:

PowerShell 101: A Quick-Start Guide to PowerShell

by Robert Sheldon

Ease your scripting pains with the flexibility of PowerShell. Learn how to use PowerShell to perform various tasks with this guide's 6 introductory lessons—complete with helpful figures, expert explanations and detailed code. Whether you're new to PowerShell or just want to brush up on the basics, this series is your scripting solution.

Order your downloadable eBook today for only $15.95*!

*Plus shipping and applicable tax.

left-brain

www.left-brain.com

Windows IT Pro

UNDERSTANDING MICROSOFT'S Virtualization TECHNOLOGIES

by Michael Otey

Navigate a maze of terminology—Hyper-V, App-V, MED-V—to determine what's best for you

Virtualization has always been a complex technology, but somehow Microsoft has found a way to even further complicate the technology by releasing its various virtualization products with similar-sounding yet nondescript names such as Hyper-V, App-V, and MED-V. To understand the role of each of these virtualization solutions and how you might use them in your business, you need to know how to navigate the maze of Microsoft virtualization terminology and methodology. Let's get started.

Server Virtualization with Hyper-V

Easily the most well-known Microsoft virtualization technology, Hyper-V is Microsoft's server-virtualization solution. Hyper-V competes head-to-head with VMware's ESX Server. Microsoft delivers Hyper-V in two ways: It's a role in Windows Server 2008 and Server 2008 R2, and it's also available free in the form of Hyper-V Server 2008 R2. The latest release of Hyper-V is typically referred to as Hyper-V 2.0.

As its name implies, Hyper-V is a hypervisor-based virtualization solution, which means that the software layer providing the virtualization support runs directly on the physical system hardware. This configuration provides a high-performance virtualization platform.

Hyper-V was originally released with Server 2008. However, the Hyper-V code that was delivered in the initial Server 2008 release was prerelease code. Later, Microsoft delivered the final Hyper-V release as a hotfix. This initial release became known as Hyper-V 1.0. The Hyper-V 1.0 release didn't support Live Migration; instead, it supported Quick Migration, a technology that incurred some downtime as virtual machine (VM) files were transferred between cluster nodes. The new Hyper-V 2.0 supports Live Migration, enabling VMs to be moved between Hyper-V hosts with no downtime. Live Migration is facilitated by a new storage technology called Cluster Shared Volumes (CSV), which allows multiple cluster nodes to access a VM file stored on a shared LUN. Live Migration is essentially the Microsoft counterpart to VMware's VMotion. Hyper-V 2.0 also provides support for up to four-way virtual SMP and up to 64GB of RAM per VM.

Hyper-V Server 2008 R2 and the Hyper-V role in Server 2008 R2 are based on the same technology. Both use the same hypervisor, and both are capable of joining a cluster and performing Live Migration. However, there are differences. One of the main technological differences is the fact that Hyper-V Server 2008 R2 must be managed remotely. There's no local GUI. Another important difference is licensing: Hyper-V Server 2008 R2 includes no licenses for any host or guest OSs. With Server 2008 and Server 2008 R2, you get at least one license for running Server 2008 and additional licenses, depending on the edition of Server 2008 you have:

- Server 2008 Standard Edition provides an additional license for one active instance of Windows running on a VM.
- Server 2008 Enterprise Edition provides for four active Windows instances running on VMs.
- Server 2008 Datacenter Edition provides for an unlimited number of active Windows instances with no additional licensing costs.

You can learn more about Server 2008 and virtualization at Microsoft's "Virtualization with Hyper-V" page (www.microsoft.com/windowsserver2008/en/us/hyperv-main.aspx), and you can download Hyper-V Server 2008

R2 at Microsoft's "Hyper-V Server 2008 R2" page (www.microsoft.com/hyper-v-server/en/us/default.aspx).

Note that Hyper-V isn't a good technology for laptops. Many laptops today are capable of running Hyper-V, but because the Hyper-V hypervisor runs directly on the hardware, you lose important mobility features such as power management and the ability to sleep and hibernate your system. Hyper-V is best suited to server virtualization. Laptops are better served by using a hosted virtualization product such as Virtual PC.

Application Virtualization with App-V

Less well known is App-V, Microsoft's application-virtualization platform, a technology that Microsoft acquired by purchasing Softricity's SoftGrid in 2006. Server virtualization and application virtualization solve very different problems. Server virtualization addresses server hardware utilization levels and server deployment and availability. Application virtualization addresses application deployment, isolation, and management.

Software running on the client system provides support for virtual applications. The client-virtualization layer provides the virtual application with a virtual copy of the system's file system, registry, and other system I/O points. When the virtual application runs, it interacts with the virtual system environment and doesn't modify the host system's physical registry and file system. This capability allows multiple applications that might normally conflict with one another to run together on the same system with no conflicts because each application runs in its own virtual environment. Likewise, it eliminates "DLL hell," where installing one application can overwrite the DLLs that another application uses. For the enterprise, the biggest App-V advantage probably lies in its no-touch application deployment. App-V is integrated with Active Directory (AD), and the administrator can assign virtual applications to users and groups, and stream those applications to end-user systems without any manual intervention.

App-V does require supporting infrastructure. The application to be virtualized runs through a process called the Microsoft Application Virtualization Sequencer, which breaks the application into pieces that can stream to desktops. The system stores the virtual applications on the System Center Application Virtualization Management Server, which is also responsible for streaming them to desktops, where the virtualization client software executes them.

One benefit of the sequencing process is that only the parts of the application that are necessary are streamed to the desktop. For example, when you run an application such as Microsoft Office (which normally requires several hundred megabytes) through the sequencer, it becomes many smaller pieces that can be individually streamed to the client. Now, when a client initially uses the application, he or she doesn't need to wait for hundreds of megabytes to stream to the system before it's useable. Instead, only the code necessary to run the executable part of the requested application streams to the client. The necessary part might be only a few megabytes, but the application will execute normally in the virtual client environment. Later, as the end user requests additional functions and features, only the code needed to execute those features will stream to the client. The virtual applications are executed on the client system, and the code streamed to the client systems remains cached there, so there's no need to restream the parts of the virtual applications that have been previously streamed to client systems.

Hyper-V isn't a good technology for laptops because you lose important mobility features such as power management and the ability to sleep and hibernate your system.

App-V is part of Microsoft's Desktop Optimization Pack (MDOP), which is available only to Software Assurance customers. You can find out more about App-V at the Microsoft Application Virtualization site (www.microsoft.com/systemcenter/appv/default.mspx).

Legacy App Compatibility with MED-V

MED-V is probably the most misunderstood product in the Microsoft virtualization lineup. Legacy application compatibility is the product's main purpose. MED-V is built on top of Microsoft's Virtual PC product, but unlike Virtual PC—in which a guest OS desktop replete with applications is presented to the user—MED-V enables the applications running in the VM to be seamlessly integrated with the user's desktop. The fact that the application is actually running on a VM is hidden from the end user. This configuration removes the complexity associated with running a product such as Virtual PC from the end user.

MED-V applications are published to users via Group Policy, and they appear like normal applications in the user's Start menu. When the user launches a MED-V application, the default policies cause the application to appear with a red border on the user's desktop. Printers defined in the host environment are available to the MED-V applications. Other desktop features (e.g., using Alt+Tab to switch between applications) are also supported for Med-V applications. MED-V is much like Windows 7's Windows XP Mode (see the next section), but MED-V is designed for enterprise usage and is centrally managed, whereas Windows XP Mode is designed for the single user.

Like App-V, MED-V is part of MDOP, which is available only to Software Assurance customers. You can find out more about MED-V at Microsoft's MDOP page (www.microsoft.com/windows/enterprise/products/mdop/med-v.aspx).

Virtual PC and Windows XP Mode

Yes, Virtual PC is alive and well, and is the basis for such technologies as MED-V and Windows XP Mode. Microsoft acquired its Virtual PC technology from Connectix in 2003, and the company has recently released a new version of Virtual PC to support Windows 7. The new version includes long-overdue support for accessing USB devices. Unlike Hyper-V, in which the virtualization hypervisor runs directly on the hardware,

Virtual PC uses a hosted virtualization model in which the virtualization software runs on a host OS. Also, unlike Hyper-V (which requires 64-bit hardware), Virtual PC can run on 32-bit and 64-bit systems.

Like MED-V, Windows XP Mode enables applications that are running in the VM to be seamlessly integrated with the user's desktop. However, Windows XP Mode also includes a full copy of XP SP3, which provides the basis for running legacy applications that might not run on Windows 7. Windows Virtual PC and Windows XP Mode are available for Windows 7's Starter, Home Premium, Professional, Enterprise, and Ultimate editions.

The new Windows Virtual PC runs only on Windows 7. If you're looking for desktop virtualization for Vista or XP, you would need the older Microsoft Virtual PC 2007, which is a free download available from Microsoft's Virtual PC 2007 page (www.microsoft.com/windows/virtual-pc/support/virtual-pc-2007.aspx). The new Windows Virtual PC is a free download from Microsoft, and you can find Virtual PC and Windows XP Mode at Microsoft's Download Windows XP Mode page (www.microsoft.com/windows/virtual-pc/download.aspx).

Virtual Server 2005 R2

Virtual Server 2005 was Microsoft's original server-virtualization technology. Virtual Server 2005 R2 is a hosted virtualization product, which means the virtualization software runs on top of a host OS such as Windows Server 2003. Now that Hyper-V is available, there's little need for Virtual Server 2005 R2, but it still fills a niche by running in certain environments that don't support Hyper-V. For example, Virtual Server 2005 R2 can run on Windows 2003. It can also run on older 32-bit hardware, whereas Hyper-V requires 64-bit hardware and a CPU that supports hardware-assisted virtualization.

The Virtual Hard Disk (VHD) format used to store VM files is compatible between Virtual PC, Virtual Server 2005 R2, and Hyper-V. You can use System Center Virtual Machine Manager (SCVMM) to manage both Hyper-V and Virtual Server 2005 R2. You can download and find out more about Virtual Server 2005 R2 at Microsoft's Virtual Server 2005 R2 page (www.microsoft.com/windowsserversystem/virtualserver).

Presentation Virtualization and the Microsoft VDI Suite

I left Remote Desktop Services (RDS) for last because RDS—formerly known as Terminal Services—doesn't really qualify as a virtualization technology. While scrambling to jump on the virtualization bandwagon, Microsoft's marketing folks tagged this technology as *presentation virtualization*. RDS is really a remote-access technology that lets a desktop—or even a window used by an application on a desktop—be displayed on a remote system. The keyboard and mouse clicks captured on the remote desktop are transmitted back to the host system, using Remote Desktop Protocol (RDP). Nothing is really virtualized; you're just operating the system remotely.

> MED-V is built on top of Microsoft's Virtual PC product, but unlike Virtual PC—in which a guest OS desktop replete with applications is presented to the user—MED-V enables the applications running in the VM to be seamlessly integrated with the user's desktop.

Virtual Desktop Infrastructure (VDI) is a technology that enables centralized management of client systems. The Microsoft Virtual Desktop Infrastructure Suite is actually something of a misnomer: The name implies that it's a product, but it's really a bundling of several Microsoft virtualization technologies, including Hyper-V for hosting desktops, SCVMM for managing the desktop VMs, System Center Operations Manager (SCOM) for monitoring hosts and VMs, System Center Configuration Manager for creating desktop images, and Windows Server RDS with its RD Session Broker and RD Gateway. Microsoft markets two versions of this product: the VDI Standard Suite and the VDI Premium Suite. The primary difference is that the Premium Suite includes App-V on top of the other products that comprise the Standard Suite. Does this sound complex and confusing? It is. None of these products is specially intended for VDI, but they can each play a different role in making VDI happen. The suites are more a way to help customers handle the licensing complexities.

Enhancements to Server 2008 R2's RD Connection Broker enable Microsoft's VDI scenario. Clients make a connection to a VM using RDP. The Server 2008 R2 RD Gateway provides web access, and the RD Connection Broker directs clients to the correct VMs. Hyper-V runs VMs with the desktop client OS. The VM's desktop is sent to the client via the RDP connection. You could think of the Microsoft VDI solution as a type of single-user terminal services. Other vendors (e.g., Citrix) offer enterprise-level management extensions to this platform.

You can find out more about the enhancements to Server 2008 R2's Remote Desktop Services at Microsoft's Remote Desktop Services page (www.microsoft.com/windowsserver2008/en/us/rds-product-home.aspx). You can find more information about Microsoft's VDI Suite at Microsoft's Desktop Virtualization page (www.microsoft.com/virtualization/en/us/products-desktop.aspx).

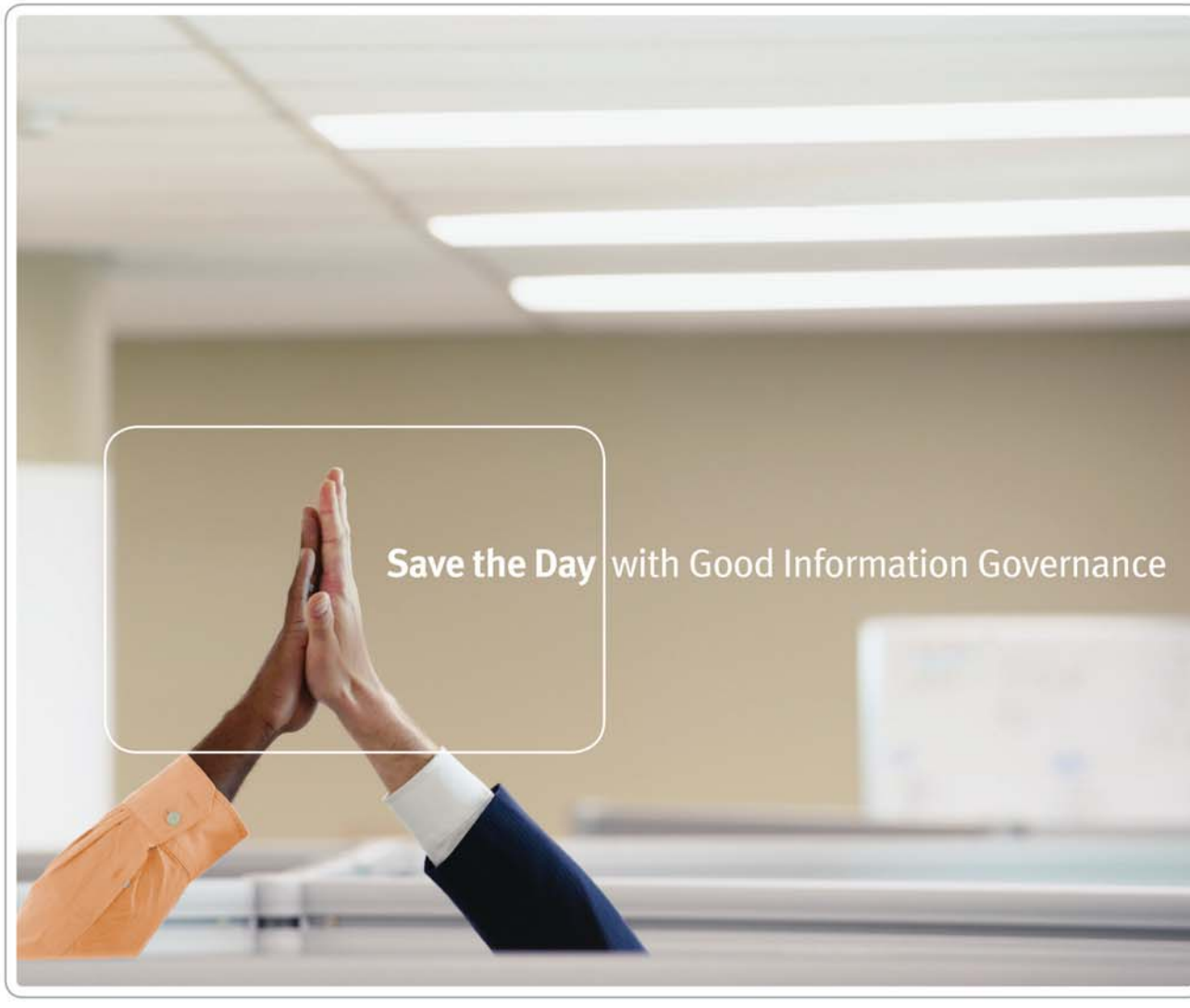
Living in the Virtual World

Virtualization has rapidly grown from a niche technology used for labs and development work to a core IT infrastructure technology. As you can see, Microsoft offers many types of virtualization technologies. Each one is designed to provide a solution to a different business problem. Hopefully, you can now find your way through the Microsoft virtualization maze.

InstantDoc ID 103245

Michael Otey
(motey@windowsitpro.com) is technical director for *Windows IT Pro* and *SQL Server Magazine* and author of *Microsoft SQL Server 2008 New Features* (Osborne/McGraw-Hill).

EMC²
where information lives®



Good information governance goes beyond simple archiving. Get there with the power of EMC SourceOne.

Cut your organization's eDiscovery costs, storage requirements, and backup windows in half* with the EMC SourceOne™ family, the most advanced and flexible portfolio of integrated e-mail management, e-discovery, and archiving products available. IT and Legal confront disparate challenges—from boosting operational efficiency to mitigating risk and ensuring litigation readiness. Now they can both embrace a single EMC® solution that takes full charge of information governance.

Learn more at www.EMC.com/SourceOneCity/Governance.

*Based on typical installation and industry analyst data.

Exchange Server Archiving for E-Discovery

With the right tool in place, you'll safely and cost-effectively navigate legal requests

by B. K. Winstead

A recent survey sponsored by Metalogix Software indicates that fully half of respondents have received a legal discovery request within the past five years. If presented with such a request, will your IT department be able to find and provide all the requested information in a timely manner?

You can help yourself out by being prepared. Have well-documented retention policies in place for email and other company documents: Don't keep what you don't need to keep, according to whichever regulations apply to your organization. And for what you must keep, for either legal or business reasons, it's a great idea to have a proper archive in place—one that can be effectively searched when an e-discovery request comes through. This buyer's guide and the product table on page 80 should help you assess the features you need in an archiving product for your Microsoft Exchange Server environment to be ready for e-discovery requests. Although there are many cloud-based services for archiving, this guide focuses only on software products.

PSTs and Other Problems

Exchange Server 2010 has introduced the personal archive feature, which is basically intended to replace PST files. It lets users decide what to archive versus what to delete. But for most legal purposes, this sort of archiving clearly won't be sufficient, as pointed out by Frank Mitchell, the product director for Metalogix Software. "People abuse email. People delete things, lose email. People create PSTs, which to us is underground archiving," Mitchell said. In other words, do you really trust your end users when legal issues are on the line?

Having some way of corralling PST data is essential because those files, too, are most likely subject to any e-discovery request—although they aren't readily searchable or even discoverable through Exchange itself. Most Exchange archiving products these days, including all of the products in the accompanying product table, have some sort of PST migration or management features that can get PST data into the archive. As Mitchell said, "We're trying to unwind that process by trying to get that data back and preserved and protected." When the PST data is part of the archive, it's searchable just like the rest of the archive data.

In addition to the PST problem, the archive might help with other potential problems. For instance, the reporting features of some archives are available with compliance-specific templates for things such as HIPAA and SOX. If they don't have pre-made templates, the product might give you the ability to create your own custom reports, but keep in mind that means more work on your end.

The ability to establish legal holds on specific archive data is a feature that's become standard. However, if you're likely to be the target of many discovery requests, you'll want advanced hold capabilities, such as the ability to create multiple, overlapping holds. In the interest of not holding things beyond the legal requirement, you can also find archives that let you expire data from the archive according to policies you configure.

The Search

Storing the data, of course, is only half the problem. You need to find what you need when you need it. And if you do get an e-discovery request, there's a good chance it won't be limited to email data—you might need to search across multiple sources, such as network file shares and SharePoint document libraries. Many of the Exchange archiving vendors offer other products for archiving such data separately from Exchange data, as well as offering products or add-ons aimed specifically at e-discovery that will federate search across these multiple sources. So, even if an email archive is all you're looking for right now, it's worthwhile to investigate the company's other offerings in case you find you need to expand later on.

Another bonus e-discovery tools can offer is a lessening of the load on the IT department. Some tools let you delegate search functions outside the IT department, which is something many companies are looking for according to Marta Farensbach, product manager for Sherpa Software. IT departments "are inundated with requests from legal, and if they can empower their legal department to do their own searches, they're all for it," Farensbach said.

Cost Now, Savings Later

You've probably heard horror stories about how much money companies have spent on e-discovery. It's sometimes less expensive just to settle the case rather than go through the hassle and cost of the discovery process. However, if you invest now in a full-featured archiving product, you're sure to be in a better position to answer any e-discovery requests that come your way—and save your company money in the long run.

InstantDoc ID 103324

B. K. Winstead (bwinstead@windowsitpro.com) is an associate editor for *Windows IT Pro* and *SQL Server Magazine*, specializing in messaging and unified communications.

ARCHIVING FOR E-DISCOVERY

Company	Product	Price	Exchange Server versions supported:					Installs on:	Type of storage used	Is the storage licensing included in the product cost?	Offline storage option (e.g., tape, DVD)	Does the interface have a GUI/ console or a web-based interface?	Does the product archive by:			Does the product archive based on Exchange journaling or another method?	Retrieval by:		The product can search:	
			5.5	2000	2003	2007	2010						Admin-defined filters	Pre-defined filters	User action		End user	Administrator	Archive	Email server
Athena Archiver 212-868-9885 www.athenaarchiver.com	Athena Archiver Electronic Discovery	As low as $3 per mailbox	✓	✓	✓	✓		Exchange server and separate server	Proprietary indexing and standard PST export formats	Yes	Optical media, AIT WORM tape	Both	✓	✓	✓	Journaling or a proprietary plug-in	✓	✓	✓	✓
C2C 508-870-2205 www.c2c.com	ArchiveOne Express	$40 per mailbox				✓	✓	Exchange server or separate server	Exchange, SharePoint, Windows file server	No	Tape, DVD	Both	✓	✓		Journaling		✓	✓	✓
CommVault 732-870-4000 www.commvault.com	Simpana	Contact vendor	✓	✓	✓	✓	✓	Exchange server or separate server	SQL Server, proprietary	Yes	Storage and hardware agnostic	Both	✓	✓	✓	Journaling in addition to processing mail out of the mailboxes/ mail store	✓	✓	✓	✓
EMC 508-435-1000 www.emc.com	EMC SourceOne Email Management	$29 per mailbox; $25 per mailbox for more than 5,000 mailboxes			✓	✓	✓	Separate server	SQL Server; supports SAN, NAS, DAS, and others	No	Tape, DVD, etc.	Both	✓	✓	✓	Journaling, scheduled archiving, user-directed archiving	✓	✓	✓	✓
GFI Software 888-243-4329 www.gfi.com	GFI MailArchiver	Prices start at $29 for 20 to 24 mailboxes		✓	✓	✓	✓	Exchange server or separate server	Embedded database, SQL Server	No	DVD	Both	✓			Journaling	✓	✓	✓	
Metalogix Software 877-450-8667 www.metalogix.com	Professional Archive Manager for Exchange	$27.50 per mailbox	✓	✓	✓	✓	✓	Separate server	SQL Server, Oracle	Yes	Any	Only a web-based interface	✓	✓	✓	Journaling, scheduled archiving	✓	✓	✓	✓
Mimosa Systems 408-970-9070 www.mimosasystems.com	Mimosa NearPoint	Starts at $40 per mailbox	✓	✓	✓	✓	✓	Separate server	SQL Server	No	None	Both	✓	✓	✓	Continuous Application Shadowing, MAPI/ journaling, VSS, Snap Manager for Exchange	✓	✓	✓	✓
Quest Software 949-754-8000 800-306-9329 www.quest.com	Quest Archive Manager	$40 per mailbox	✓	✓	✓	✓	✓	Separate server	SQL Server, others such as NetApp	Yes	Yes	Only a web-based interface	✓	✓	✓	Journaling, archiving policies	✓	✓	✓	
RedGate Software 866-997-0385 800-169-7433 www.red-gate.com	Exchange Server Archiver	$30 per mailbox			✓	✓		Exchange server or separate server	Flat file system	No	Any	Both	✓			MAPI	✓	✓	✓	✓
Sherpa Software 412-206-0005 800-255-5155 www.sherpasoftware.com	Archive Attender	Contact vendor	✓	✓	✓	✓	✓	Exchange server or separate server	Disk storage on any UNC path location	Yes	None	Only a GUI/ console	✓		✓	Journaling, MAPI-based mailbox archiving	✓	✓	✓	✓
Sunbelt Software 727-562-0101 888-688-8457 www.sunbeltsoftware.com	Sunbelt Exchange Archiver	Volume-based license starts at $1,895 with 50 mailbox minimum		✓	✓	✓		Exchange server or separate server	SQL Server	Yes	Yes	Both	✓		✓	MAPI call to Exchange store mailboxes	✓	✓	✓	✓
Symantec Corporation 800-745-6054 www.symantec.com	Enterprise Vault	$50 to $100 per mailbox		✓	✓	✓		Separate server	SQL Server	No	Tape, optical media, virtual tape library	Both	✓	✓	✓	Journaling, MAPI-based mailbox archiving	✓	✓	✓	✓

Editor's Note: The information in this Buyer's Guide is supplied by the vendors. Some vendors you might expect to see in this Buyer's Guide either didn't have a product that matched the criteria for the guide or didn't respond to our requests for product information.

	What criteria can the product search on?										Compliance features:				Reporting features:			Additional products or add-ons the company offers that work with this product for e-discovery
Across multiple servers/ information stores	Keyword (full-text)	Size	Date range	User/ group	Subject	Sender	Quotas	Attachment type	Customizable rules	Deleted items	Litigation holds	Multiple holds	Nonerasable/ nonrewritable storage	Variable, configurable retention periods for users/groups, keywords, subject, etc.	Customizable reports	Storage data reports	Compliance-specific templates:	
✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓		✓	SOX, SEC, HIPAA, Financial Industry Regulatory Authority (FINRA)	Policy Wall add-on lets users create custom rules, such as setting retention policies, to apply to every message
✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓		SOX, HIPAA	None
✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		None
✓	✓	✓	✓	✓	✓	✓		✓	✓		✓	✓	✓	✓	✓	✓		Optional components let customers consolidate a specific subset of archived email that might be relevant to an e-discovery request; a supervisory add-on allows for discovery of messages on an on-going basis
	✓	✓	✓	✓	✓	✓					✓		✓	✓				None
✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		File and SharePoint archiving, with single instancing and full e-discovery functionality across all three types
✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		Case management, SharePoint archiving, file archiving, tiered storage capability, monitoring/ surveillance, storage management
✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓		✓		MessageStats, Recovery Manager for Exchange
✓	✓																	None
✓	✓	✓	✓	✓	✓	✓		✓		✓	✓				✓	✓		Discovery Attender for Exchange, Mail Attender
✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		None
✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓		Discovery Accelerator, Compliance Accelerator, open API with integration to leading discovery solutions

INSIGHTS FROM THE INDUSTRY

Should You Get a DROID?

"iDon't have a real keyboard … iDon't run simultaneous apps … iDon't take 5-megapixel pictures …"

These are the first three points in a powerful smackdown ad campaign for the Motorola DROID, clearly targeting the iPhone. The message is clear: Where the iPhone lacks, DROID excels. (Visit tinyurl.com/ygby6ps for a sample ad spot.)

Most of us are probably yawning at yet another iPhone comparison, but the strategy has paid off. Sales for the DROID are estimated at 700,000 already and are expected to hit 1 million by the end of the year. But does the DROID live up to the hype? And how does it stand up to the expectations of enterprises? Let's take a look at these questions in more depth.

What the DROID Offers

Many of the DROID's more exciting features have been publicized in the ubiquitous online and TV ads—support for simultaneous apps, a 5-megapixel camera, and a removable battery. The DROID's 3.7" screen displays 854×480 pixels, making it one of the best resolutions available on a smartphone. Performance appears to be comparable to competing devices—550MHz processor, 256MB RAM, 16GB memory. (Full specs at tinyurl.com/DROIDspecs.)

Above all, the DROID is available on Verizon's network. This is probably its biggest selling point, considering Verizon's network is widely accepted as the most reliable network, offering the greatest national 3G coverage (as recent ads targeting AT&T have been quick to point out).

Above all, the DROID is available on Verizon's network. This is probably its biggest selling point, considering Verizon's network is widely accepted as the most reliable network, offering the greatest national 3G coverage.

New Android 2.0 Features

Android 2.0 may not be a huge evolution from previous versions, but there are a few noticeable enhancements. First off, Android 2.0 supports multiple Gmail and Exchange accounts, letting you create a universal inbox for all your accounts. Another feature is Quick Contact, which lets you tap any contact and have a window pop up with all the different ways you can communicate with that contact (e.g., social media, email, view a map of the contact's address). While it hardly offers the tight social networking integration of devices such as the Palm Pre or Motorola CLIQ, it's a good blend for people who use various social networks but don't want a device that revolves around them.

Another terrific benefit of the Android 2.0 is turn-by-turn GPS navigation, which—if you're like me—is essential to survival.

Android and the Enterprise

Can you use the DROID and other Android phones in the enterprise? Sure. Do they offer the kind of security and management features out-of-the-box that BlackBerry devices and Windows Mobile phones have? Certainly not. Android supports ActiveSync but can't sync Tasks, To-Do Lists, and Memos. Additionally, Android doesn't allow for remote wipe (in the event of a lost or stolen device) or remote provisioning and setup. But these concerns can be easily conquered: Many mobile management products today support Android devices, granting remote wipe/provisioning and a lot more. So, assuming your organization has a multi-platform mobile management solution in place, using the DROID should be no big obstacle.

Closing Thoughts

The DROID is a strong contender. Most of the Android phones currently in the market are somewhat lackluster, and Windows Mobile is suffering more and more in the marketplace. If your organization doesn't support a variety of devices, push for it-smartphones are a big source of individual expression, especially for VIPs. Great network, snazzy device, and it's not an iPhone. Being a DROID user is pretty cool in my book.

—Brian Reinholz
InstantDoc ID 103236

Tony Redmond's Top 10 Things About Exchange 2010

At Microsoft Exchange Connections last November in Las Vegas, Exchange expert Tony Redmond delivered a keynote address entitled "Top 10 Things You Need to Know About Exchange 2010." With Microsoft's announcement the same week at TechEd Europe in Berlin about the immediate availability of Exchange Server 2010, Redmond's topic was well chosen, and the keynote was well attended. For those who couldn't be there, here is Redmond's top 10 list.

1. Exchange 2010 is release 3.2 of Exchange Server. What Redmond means by this statement is that Exchange 2010 is the second version of the third generation of Exchange. The first generation includes the versions before Exchange 2000; the second generation is Exchange 2000 and Exchange 2003. The third stage began with Exchange 2007, which marked a fundamental change in the architecture of Exchange organizations. As the second release of this generation, Exchange 2010 should be past the initial growing pains that such drastic changes bring about.

2. First fundamental refresh of the Information Store since 1996. The improvements or upgrades to the Store include a larger database page size (up to 32KB from 8KB in Exchange 2007) and improved I/O, which is more sequential and less random. Because of these improvements, single instance storage (SIS) has been eliminated as no longer important. Also, storage groups are gone; management is intended to be by the database.

3. New software-based approach to high availability. High availability is built in to Exchange 2010 through Database Availability Groups (DAGs), which let you replicate databases to multiple servers with automatic failover in the event of problems. This architecture also introduces the concept of incremental deployment—that is, you can add servers and mailboxes as you need them; you don't have to plan everything before you begin.

4. Hosted Exchange and on-premises are equal (almost). Exchange 2010 was developed from the beginning to be scalable as a cloud-based solution as well as deployable in your on-premises data center, and it has received extensive testing through Microsoft's online initiatives. Therefore, it's clearly ready and able to be successfully deployed as a hosted service, although a few features might still be available only with on-premises deployments.

5. No upgrade path, must install on fresh hardware. I suspect this is a point that still might be unpopular with many users. Redmond explained that because you need to carefully consider your underlying OS, it makes sense to do fresh installs rather than upgrades. Exchange 2007 had the same situation; however, keeping in mind that this version is within the same generation, no doubt many admins expected the opportunity of an in-place upgrade at least if they were already on Exchange 2007. No such luck.

> Be careful assiging roles, or you could end up locking yourself out of the management areas you need to be in, with no way back!

6. More fully developed message compliance features. Compliance features in Exchange 2010 build on the good start of Exchange 2007 and provide a more feature-rich and customizable experience. Although the new personal archive isn't specifically a compliance feature, it can be used in conjunction with retention policies and rules to aid in better mailbox management. Improvements to the transport dumpster (what Redmond called Dumpster 2.0) let it keep track of all edits and deletions for better visibility of end user actions. And Exchange 2010 also introduces cross-mailbox search capability, which is a great first step toward e-discovery.

7. Role-Based Access Control (RBAC) replaces ACL-based permissions. With RBAC, users see in the GUI only functions they have permissions to perform; this restriction applies also to PowerShell-based management and the ability to use only cmdlets that are authorized for assigned roles. Redmond did mention the need to be careful assigning roles, or you could end up locking yourself out of the management areas you need to be in, with no way back.

8. PowerShell 2.0. As you've no doubt seen, Exchange 2010 adds many new features, and that means many new Windows PowerShell cmdlets to manage things—hundreds, in fact. Additionally, PowerShell 2.0 adds remote management capability so you no longer need to work locally to get the job done. Redmond warned to be sure to test your PowerShell 1.0 scripts because some cmdlets have been removed and some might work differently in PowerShell 2.0.

9. Exchange Control Panel (ECP). You can still manage Exchange 2010 with Exchange Management Console (EMC) and Exchange Management Shell (EMS), but now you also have the option to use the browser-based ECP, giving you additional remote management capabilities. You can also use ECP to delegate some functions to end users, such as simple password resets—and thereby save lots of calls to the Help desk.

10. And lots more. OK, Tony, I think you're cheating a little with this one, but in a well-meaning way. After all, there's a lot of worthy stuff to talk about with Exchange 2010. Redmond's list of more items included such things as MailTips, Exchange Web Services as API, UM upgrades such as personal attendants, and of course the big improvements in Outlook Web App (formerly Outlook Web Access, but still OWA).

—B. K. Winstead

InstantDoc ID 103132

1&1 Dynamic Cloud Server

FLEXIBLE

Easy to configure. Always adjustable.

1&1® DYNAMIC CLOUD SERVER

The flexible individual server solution adaptable to your needs! A virtual server environment with full root access – adjust the processor core, RAM, and/or hard disk space at any time. Prices will be reflected accordingly.

Basic Configuration:

- **1 AMD Opteron™ 2352 Core Processor** (up to 4 cores available)
- **1 GB RAM** (up to 15 GB RAM available)
- **100 GB Hard Disk Space** (up to 800 GB available)

All Configurations Include:

- **2000 GB Traffic**
- **Full Root Access**
- **Windows Server 2008 R2 Standard**
  Available as an add-on, additional fees apply.
- **Parallels Plesk Panel 9**
- **24/7 Toll-Free Support**

Basic Configuration:
~~$49.99~~ per month

Special Offer:
3 Months FREE!*

EPA GREEN POWER PARTNER

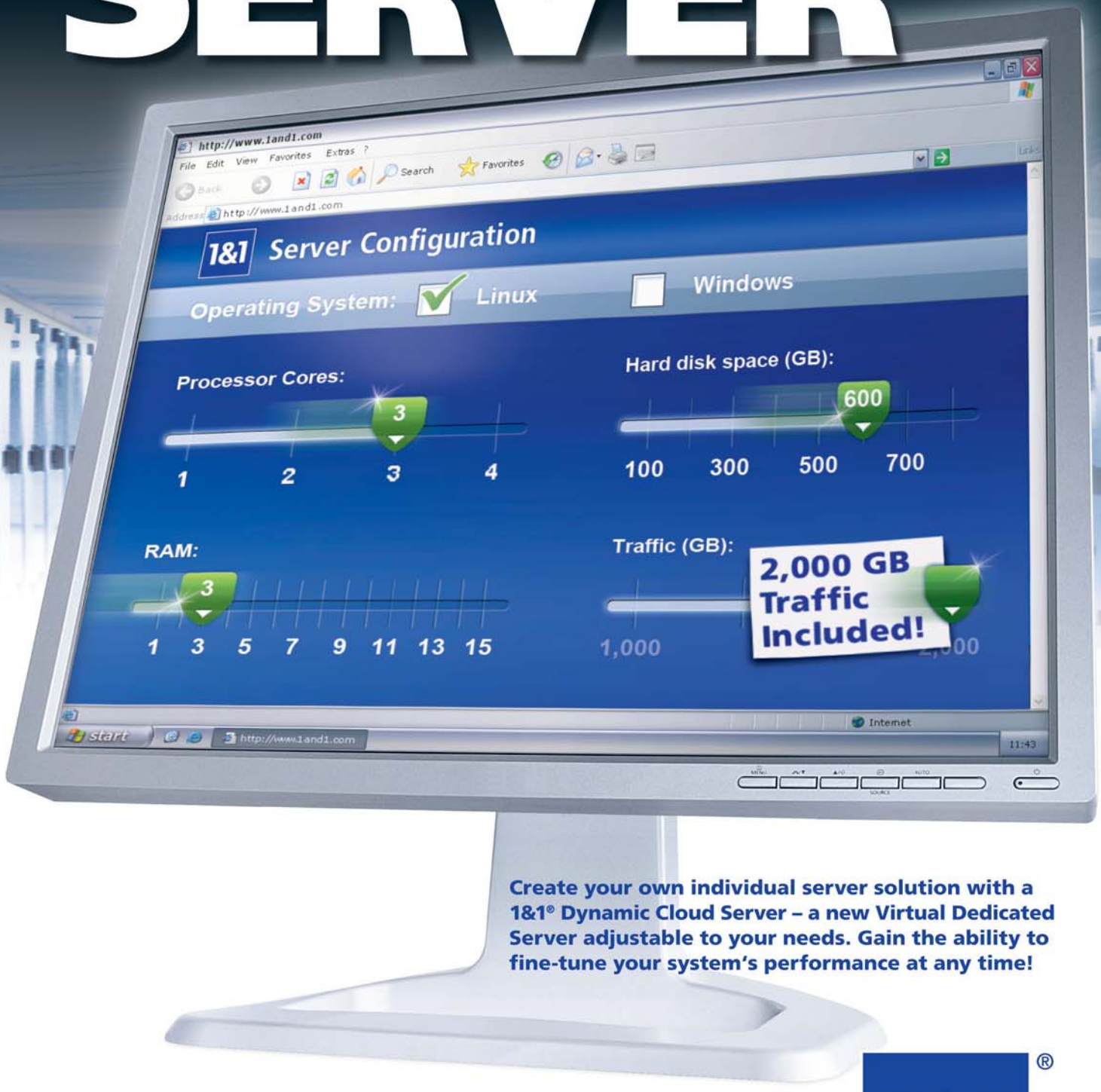
*3 months free offer applies to basic configuration only. 12 month minimum contract term and set up fee apply. Visit website for full promotional offer details. Program and pricing specifications and availability subject to change without notice. 1&1 and the 1&1 logo are trademarks of 1&1 Internet AG, all other trademarks are the property of their respective owners.

MEMBER OF united internet

1-877-GO-1AND1

NEW!

SERVER



Create your own individual server solution with a 1&1® Dynamic Cloud Server – a new Virtual Dedicated Server adjustable to your needs. Gain the ability to fine-tune your system's performance at any time!

Visit our website for more special offers!

www.1and1.com

1&1®

Hire Better Employees with This 5-Step Process

HR reps and hiring managers generally agree that hiring and firing are the two worst parts of the business. Fortunately, sharpening your hiring procedure can kill two birds with one stone: reduce the difficulty and guessing in hiring and decrease the frequency of firing.

How? By injecting logic deep into the heart of the hiring process. Consider this innovative five-step hiring procedure from Platinum Solutions.

The 5-Step Process

Here is the five-step process that Platinum Solutions uses:

1. Online technical test. All applicants take an online technical test to measure basic competencies in the industry and technologies relevant to the position. According to Laila Rossi, CEO of Platinum Solutions, this test cuts out 50 to 60 percent of applicants. Talk about reducing the strain involved in sifting through hundreds of resumes, a process fraught with unqualified candidates slipping through the cracks and excellent candidates weeded out.

2. Cognitive test. The second step is a cognitive test to measure the logic and critical thinking skills of candidates. Simply put, you want smart people in your organization.

3. Face-to-face technical interview. In this stage, a trained interviewer will ask specific questions to gauge technical capabilities. Please note that this interview doesn't focus on experience, but current skill and competency. Hearing about deployments that a person managed or examples of when he or she handled a crisis situation might be interesting, but these anecdotes do little to prove one's competency. A far greater test is to ask complex, targeted questions, then judge the depth and value of the answer that the candidate gives. It's absolutely essential that a well-trained and technically savvy individual conduct this interview.

4. Top grading interview. The "top grading" interview (as Rossi puts it) is potentially the most interesting piece of the hiring process. In this step, a hiring manager (or trained interviewer) goes through an employee's entire work history in a very probing manner. The interviewer asks questions such as, "What role were you hired to fill?" and "What were your experiences with other staff?" and "What staff members did you disagree with and why?" Because the interviewee knows that the company will perform spot reference checks on any employee (not just employers) in previous organizations, he or she has no choice but to be honest. And given the in-depth nature of the interview, no interviewee can prepare enough canned answers to not easily be spotted.

"You're giving people truth serum," said Rossi. "When you ask so many questions about so many people on their team, that's truth serum. I get people who just say, 'Why did I even talk about that?' That's when you know it's a good interview."

5. Reference check. The last step is a reference check--not with the favorite employer, teacher, and uncle that the employee provides information for, but with the fellow coworkers and managers that stick out from the top grading interview. Through these calls, you discover the nitty gritty of how the employee works with others, what his or her strengths and weaknesses are, and whether he or she is a good fit for your organization.

The Result

The end result of this process is that you're left with a candidate who you know, without a doubt, has the technical competencies, the intellect, and proven work history to succeed. You essentially isolate any biases based on personalities. "You [avoid] those friendly interviews where they have something in common, and the interview's over within 10 minutes. That's a waste of time, and that's how you get those faulty hires," Rossi said.

That's not to say personality isn't still important, though. But keep it in a business context. "You want to make sure a person can establish rapport—maintain eye contact. I definitely get people who stare down and twiddle their thumbs or stare at the ceiling. Those are not people we would typically hire," Rossi said.

Not the Best Process for All Jobs

Granted, this five-step process isn't the best hiring process for all types of employees. For low-level positions in non-critical roles, you might opt for a more basic, personality-based interview process. But for the positions that play key roles in driving your business, you need the most intelligent, capable people you can find. And given that few organizations use processes like this, I have little doubt that there are numerous excellent candidates in your area that simply haven't surfaced to your awareness.

—Brian Reinholz

InstantDoc ID 103129

For detailed information about products in this issue of *Windows IT Pro*, visit the web sites listed below.

COMPANY/URL	PAGE
1&1 Internet www.1and1.com	12, 13, 84, 85
Advaiya www.platformvision.com	8B
Appassure Software www.appassure.com	8B
Binary Tree www.binarytree.com/Exchange2010	24B
EMC Corporation www.EMC.com/SourceOneCity/Governance	78
IBM Corporation www.ibm.com/flexible	Cover 2
Microsoft Corporation www.itseverybodysbusiness.com/optimize	Cover 4
Microsoft Corporation www.microsoft.com/exchange	24B
Novell Inc. www.novell.com	8B
Privacyware www.privacyware.com	86
Steeleye Technology www.steeleye.com	8B
Sunbelt Software Inc. www.TestDriveVipre.com	Cover 3
SharePointPro 2010 Summit & Expo www.SharePointProSummit.com	40B
VirtualizationPro 2010 Summit & Expo www.VirtualizationProSummit.com	16, 72B
Windows IT Pro www.windowsitpro.com	4, 10, 20, 74

VENDOR DIRECTORY

The following vendors or their products are mentioned in this issue of *Windows IT Pro* on the pages listed below.

Athena Archiver	80	
Bomgar	64	
C2C	80	
CommVault	80	
DeskCenter	64	
EMC	80	
Ensim	69	
GFI Software	80	
Kerio Technologies	65	
ManageEngine	69	
Metalogix Software	80	
Mimosa Systems	67, 80	
Motorola	82	
NetIQ	69	
NewSoftwares.net	64	
Platinum Solutions	84	
Quest Software	69, 80	
Red Gate Software	80	
Sendio	68	
Sherpa Software	65, 79	
Sunbelt Software	80	
Verizon Wireless	84	
VMware	64	

DIRECTORY OF SERVICES | WINDOWS IT PRO NETWORK

Search our network of sites dedicated to hands-on technical information for IT professionals.
www.windowsitpro.com

Support

Join our discussion forums. Post your questions and get advice from authors, vendors, and other IT professionals.
www.windowsitpro.com/forums

News

Check out the current news and information about Microsoft Windows technologies.
www.wininformant.com

EMAIL NEWSLETTERS

Get free news, commentary, and tips delivered automatically to your desktop.

- *asp.netNOW*
- *Exchange & Outlook UPDATE*
- *SharepointPro Connections UPDATE*
- *Security UPDATE*
- *SQL Server Magazine UPDATE*
- *DevConnections UPDATE*
- *Windows IT Pro UPDATE*
- *Windows Tips & Tricks UPDATE*
- *WinInfo Daily UPDATE*

www.windowsitpro.com/email

RELATED PRODUCTS

Custom Reprint Services

Order reprints of *Windows IT Pro* articles. Diane Madzelonka at Diane.madzelonka@penton.com.

Super CD/VIP

Get exclusive access to all of our print publications, including *Windows IT Pro,* via the new, banner-free VIP Web site.
www.windowsitpro.com/sub/vip

Article Archive CD

Access every article ever printed in *Windows IT Pro* magazine since September 1995 with this portable and speedy tool.
www.windowsitpro.com/sub/cd

SQL SERVER MAGAZINE

Explore the hottest new features of SQL Server, and discover practical tips and tools.
www.sqlmag.com

ASSOCIATED WEBSITES

DevProConnections

Discover up-to-the-minute expert insights, information on development for IT optimization, and solutions-focused articles at DevProConnections.com, where IT pros creatively and proactively drive business value through technology.
www.devproconnections.com

Office & SharePoint Pro

Dive into Microsoft Office and SharePoint content offered in specialized articles, member forums, expert tips, and Web seminars mentored by a community of peers and professionals.
www.officesharepointpro.com

NEW WAYS TO REACH *WINDOWS IT PRO* EDITORS:

LinkedIn: To check out the *Windows IT Pro* group on LinkedIn, sign in on the LinkedIn homepage (www.linkedin.com), select the Search Groups option from the pull-down menu, and use "Windows IT Pro" as your search term.

Facebook: We've created a page on Facebook for *Windows IT Pro*, which you can access at: http://tinyurl.com/d5bquf. Visit our Facebook page to read the latest reader comments, see links to our latest web content, browse our classic cover gallery, and participate in our Facebook discussion board.

Twitter: Visit the *Windows IT Pro* Twitter page at www.twitter.com/windowsitpro.

Windows IT Pro

by Jason Bovberg

PRODUCT OF THE MONTH

Our favorite product announcement this month comes from KneeBouncers. "Toddlers, get ready to bang away! KneeBouncers introduces a brand new, innovative website that gives babies and toddlers the opportunity to play on the Internet, without the use of a mouse." For many of you, the image of children banging away at a keyboard reminds you of your end users, but this product is purely for the kids. "KneeBouncers offers 17 games for little ones—for hours of entertainment. All with the 'cause and effect' idea: A hit of the key, and something interesting happens on screen." Yeah, you're still thinking of your end users, aren't you? For more information, visit the KneeBouncers website at www.kneebouncers.com.

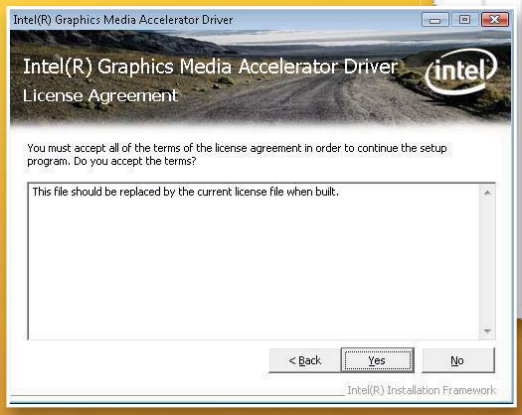


Figure 1: Free-for-all!

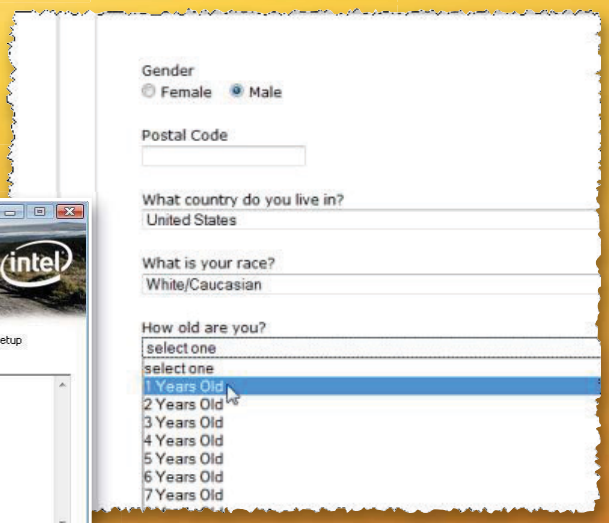


Figure 2: Perhaps a good candidate for KneeBouncers?

User Moment of the Month

I started with an IT team a few years ago, managing a few remote branch offices, and during one of my first weeks on the job, a user called me with a problem. To troubleshoot, I asked her to check out a setting on her computer. She put the phone down, and I heard her walking away. Each time I gave her instructions, she would walk to her system on the other side of a large room. I told her the troubleshooting process might be less time-consuming if she could use a phone closer to the system. She laughed, transferred me to the phone on the same desk as the troubled system, and things went much more smoothly.

—Adam

SEND US YOUR INDUSTRY HUMOR!

Email your industry humor, scandalous rumors, funny screenshots, favorite end-user moments, and IT-related pics to rumors@windowsitpro.com. If we use your submission, you'll receive a ***CTRL+ALT+DEL GIFT.***

February 2010 issue no. 186, *Windows IT Pro* (ISSN 1552-3136) is published monthly. *Windows IT Pro,* 221 E. 29th St., Loveland, CO 80538, (800) 793-5697 or (970) 663-4700. Sales and Marketing Offices: 221 E. 29th St., Loveland, CO 80538. Advertising rates furnished upon request. Periodicals Class postage paid at Loveland, Colorado, and additional mailing offices. **POSTMASTER: Send address changes to *Windows IT Pro,* 221 E. 29th St., Loveland, CO 80538. SUBSCRIBERS:** Send all inquiries, payments, and address changes to *Windows IT Pro,* Circulation Department, 221 E. 29th St., Loveland, CO 80538. Printed in the USA. BPA Worldwide Member.

Kiss your antivirus bloatware goodbye

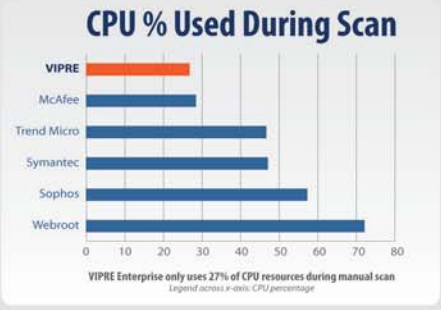
Special Competitive Upgrade: 50% Discount!

VIPRE® ENTERPRISE

TEST DRIVE

Next Generation of Total Malware Protection

The configurable Command Center puts all the information you need in one place. Manage individual agents, quarantines, threats, and more.



How does your current software compare? VIPRE Enterprise scans at a brisk 13.95 MB/sec and uses just 27% of CPU and 50 MB of RAM. In idle, it uses a mere 13.3 MB RAM with a disk footprint of just 113 MB. You'll hardly notice it's running!

Sunbelt Software

Until now, antivirus engines have been Frankensteins, bolted together from bits and pieces of different products. They're slow, full of bugs, and hard to manage.

VIPRE Enterprise is a revolutionary new approach. It's built from scratch as the all-in-one antivirus, antispyware, anti-rootkit solution that gives you complete endpoint malware protection ***without hogging resources!*** It's fast, powerful, and easy.

Plus, advanced anti-malware technology protects your system against the new wave of malware threats. No more juggling multiple programs. No more dealing with user complaints about slow workstation performance.

- **COMPLETE!** All-in-one protection from today's malware.
- **FAST!** High-performance and low impact on system resources.
- **EASY!** Manage everything easily from one command screen.
- **RELIABLE!** Configurable, real-time monitoring technology.
- **AFFORDABLE!** Ask for a quote with our 50% competitive upgrade discount!

Why struggle with slow resource hogs when you can manage ALL your malware threats with one fast, easy application?

Curious? Download your FREE copy of VIPRE Enterprise and give it a test drive.

When you compare VIPRE Enterprise to Symantec, McAfee, Trend Micro or whatever antivirus program you're using, **you WILL want to switch!** Don't worry, though.You can get VIPRE Enterprise with a **50% competitive upgrade discount!**

Compatible with Windows 7

BEST IN TECH 2009 Computer Administrator

Windows IT Pro 2009 Community Choice GOLD

vb 100 VIRUS virusbtn.com

Download VIPRE Enterprise today and get your own home version of VIPRE to keep FREE as our gift to you!

Download now: www.TestDriveVipre.com

Sunbelt Software Tel: 1-888-688-8457 or 1-727-562-0101 Fax: 1-727-562-5199 www.SunbeltSoftware.com sales@sunbeltsoftware.com

Microsoft

Productivity & Efficiency. Any time. Any place.

Don't let anyone tell you that freedom comes at the cost of control. With Windows® 7 and Windows Server® 2008, users get more powerful search, smoother multitasking and the ability to work from virtually anywhere without a VPN. Add System Center and the Microsoft® Desktop Optimization Pack, and you get more automated PC management and increased control over your environment. Control for you and flexibility for your users. Optimized may not be a strong enough word.

To learn more about how desktop optimization can drive efficiencies go to **itseverybodysbusiness.com/optimize**

Snap this tag to get the latest news on desktop optimization or text OPTIMIZE to 21710

Get the free app for your phone at **http://gettag.mobi**

Because it's everybody's business